PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-115838

(43)Date of publication of application : 18.04.2003

(51)Int.Cl. H04L 9/32

(21)Application number : 2002-186588

(22)Date of filing : 26.06.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : NAKANO TOSHIHISA
OMORI MOTOJI
TATEBAYASHI MAKOTO

(30)Priority

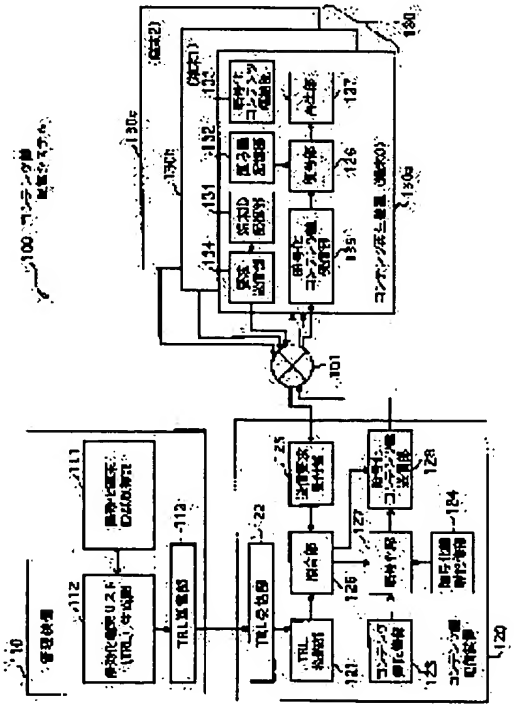
Priority number : 2001233223 Priority date : 01.08.2001 Priority country : JP

(54) ENCRYPTED DATA DELIVERY SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide technology for suppressing the data amount of information (TRL) for specifying a plurality of terminals and a terminal to be invalidated in a system composed of a plurality of terminals, a distributor for delivering data only to terminals except for the terminal to be invalidated and a management device for generating the TRL.

SOLUTION: A management device 110 generates the TRL composed of data expressing the terminal ID of all invalidated terminals having a common bit stream in one part of the terminal ID only with the position and value of the bit stream in one part and transmits the TRL to a contents key distributor 120. Each of terminals 130 holds the terminal ID containing a maker class and a serial number or the like and the distribution of the contents key is requested by sending the terminal ID to the contents key distributor 120. While referring to the TRL, the contents key distributor 120 decides whether the terminal ID sent from the terminal is the terminal ID of the invalidated terminal or not and when the sent terminal ID is not the terminal ID of the invalidated terminal, the contents key is enciphered and transmitted to that terminal.



THIS PAGE BLANK (USPTO)

LEGAL STATUS

[Date of request for examination]	07.02.2005
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－115838
（P2003－115838A）
(43)公開日　平成15年４月18日(2003.4.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ　５Ｊ１０４

審査請求　未請求　請求項の数36　ＯＬ　（全 30 頁）

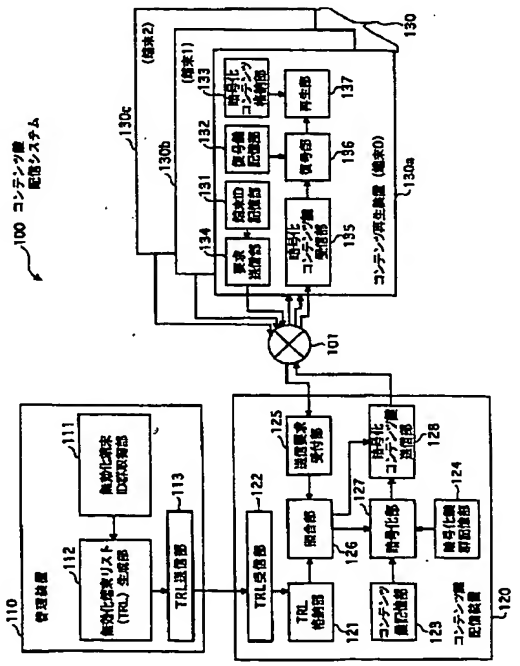
(21)出願番号　特願2002－186588(P2002－186588)
(22)出願日　平成14年６月26日(2002.6.26)
(31)優先権主張番号　特願2001－233223(P2001－233223)
(32)優先日　平成13年８月１日(2001.8.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　中野　稔久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　暗号化データ配信システム

(57)【要約】
【課題】　複数の端末と、無効化すべき端末を特定する情報（ＴＲＬ）を取得して無効化すべき端末以外の端末に対してのみデータを配信する配信装置と、ＴＲＬを生成する管理装置から構成されるシステムにおけるＴＲＬのデータ量を抑える技術を提供する。
【解決手段】　管理装置１１０は、端末ＩＤ中の一部のビット列が共通な全ての無効化端末の端末ＩＤを、その一部のビット列の位置及び値のみで表現したデータからなるＴＲＬを生成してコンテンツ鍵配信装置１２０に送信する。各端末１３０はメーカー種別やシリアル番号等を含む端末ＩＤを保持しており、コンテンツ鍵配信装置１２０に対し端末ＩＤを送ってコンテンツ鍵の配信要求を行う。コンテンツ鍵配信装置１２０は、ＴＲＬを参照し、端末から送られた端末ＩＤが無効化端末の端末ＩＤか否かを判定し、送られた端末ＩＤが無効化端末の端末ＩＤでなければその端末にコンテンツ鍵を暗号化して送信する。



1

【特許請求の範囲】

【請求項１】　暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして１以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、

前記管理装置は、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、

生成された前記無効化端末特定情報を出力する出力手段とを有し、

前記暗号通信装置は、

前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、

端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、

前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、

前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする暗号通信システム。

【請求項２】　前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、

所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、

端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、

前記判定手段は、

前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、

当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項１記載の暗号通信システム。

2

【請求項３】　前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、

所定ビット数のビット列である代表値情報と、所定ビット数のマスクフラグとを対応付けて１組以上含んでおり、

端末識別子中の部分のうち各マスクフラグにおけるビット値が１である部分の値が、当該マスクフラグに対応する代表値情報における当該部分の値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、

前記判定手段は、

前記無効化端末特定情報に含まれる各マスクフラグについて、前記端末識別子受信手段により受信された端末識別子と当該マスクフラグとの論理積と、当該マスクフラグに対応する代表値情報と当該マスクフラグとの論理積とが一致するか否かを検査し、

当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項１記載の暗号通信システム。

【請求項４】　前記無効化端末特定情報生成手段は、前記無効化端末特定情報に所定ビット数の孤立値情報を含めて生成し、

前記無効化端末特定情報は、更に前記孤立値情報と同一の値を有する端末識別子をも、無効化すべき端末装置として特定する情報であり、

前記判定手段は更に、

前記端末識別子受信手段により受信された端末識別子と、前記無効化端末特定情報に含まれる孤立値情報とが一致する場合にも、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項３記載の暗号通信システム。

【請求項５】　前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、

ビット桁数を示す有効上位桁情報と、当該ビット桁数分のビット列の値を示す値情報とを対応付けて１組以上含んでおり、

端末識別子中の最上位ビットから各有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と同一である全

ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、
前記判定手段は、
前記無効化端末特定情報に含まれる各有効上位桁情報について、前記端末識別子受信手段により受信された端末識別子中の最上位ビットから当該有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と一致するか否かを検査し、
当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項１記載の暗号通信システム。
【請求項６】　前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、
前記無効化端末特定情報生成手段は、前記所定ビット数をＮとすると、前記端末識別子取得手段により取得された端末識別子のうち最上位ビットからＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値を１以上特定し、各Ｘの値について、当該条件に係る２の（Ｎ－Ｘ）乗個の端末識別子を、Ｘなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからＸビットの部分のビット列の値を示す値情報とでもって包括的に表現したデータ形式を用いて前記無効化端末特定情報を生成することを特徴とする請求項５記載の暗号通信システム。
【請求項７】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、
前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項６記載の暗号通信システム。
【請求項８】　前記各端末装置を識別する各端末識別子は、当該端末識別子中の前記製造者を示すビット列に続く上位の所定数のビット列で、当該端末装置が如何なる種別の製品に属するかを示すことを特徴とする請求項７記載の暗号通信システム。
【請求項９】　前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、
前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、
前記暗号通信装置は、
全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、
前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを有し、
前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、
前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、
前記端末装置は、
暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、
前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することを特徴とする請求項７記載の暗号通信システム。
【請求項１０】　前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、
所定ビット数のビット列中の一部分の値及び当該部分を特定する包括情報を１以上含み、かつ、所定ビット数の例外情報を１以上含んでおり、
端末識別子中の部分のうち各包括情報により特定される部分が当該包括情報により特定される値と同一である全ての端末識別子のうちから、前記各例外情報と同値である端末識別子を除いたものの全てを、無効化すべき端末装置として特定する情報であり、
前記判定手段は、
前記端末識別子受信手段により受信された端末識別子が、前記無効化端末特定情報に含まれるいずれかの包括情報により特定される部分において当該包括情報により特定される値と一致するか否かを検査し、
当該検査において一致した場合には、当該受信された端末識別子が前記無効化端末特定情報に含まれるいずれかの例外情報と同値である場合を除いて、当該端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項１記載の暗号通信システム。
【請求項１１】　前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、
前記無効化端末特定情報生成手段は、前記所定ビット数をＮとすると、
前記端末識別子取得手段により取得されたいずれかの端末識別子の最下位ビットのみ反転したＮビットのビット列であって、当該端末識別子取得手段により取得された他のいずれかの端末識別子とも値が同一でないという条

件を満たすビット列を、前記例外情報と定めるとともに、当該ビット列を端末識別子とみなし、
前記端末識別子取得手段により取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットからＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値で、かつ、Ｎ未満であるＸの値を、１以上特定し、特定した各Ｘの値について、当該Ｘの値と、当該条件に係る２の（Ｎ－Ｘ）乗個の端末識別子の最上位ビットからＸビットの部分のビット列の値とを特定する情報を前記包括情報と定めることにより前記無効化端末特定情報を生成することを特徴とする請求項１０記載の暗号通信システム。

【請求項１２】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、
前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項１１記載の暗号通信システム。

【請求項１３】　前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、
前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、
前記暗号通信装置は、
全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、
前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを有し、
前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、
前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、
前記端末装置は、
暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、
前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することを特徴とする請求項１２記載の暗号通信システム。

【請求項１４】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、
前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項１記載の暗号通信システム。

【請求項１５】　前記複数の端末装置は各々固有の復号鍵を保持しており、
前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段を有し、
前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて通信データを暗号化して送信し、
前記端末装置は、暗号通信装置から送信された通信データを自端末装置固有の前記復号鍵を用いて復号することを特徴とする請求項１記載の暗号通信システム。

【請求項１６】　前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、
前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行うことを特徴とする請求項１記載の暗号通信システム。

【請求項１７】　前記出力手段は、記録媒体を装着可能な装着部を有し、装着された記録媒体に前記無効化端末特定情報を記録することにより前記出力を行い、
前記無効化端末特定情報取得手段は、前記記録媒体を装着可能であり、装着された記録媒体から前記無効化端末特定情報を読み出すことにより前記取得を行うことを特徴とする請求項１記載の暗号通信システム。

【請求項１８】　複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき１以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、
前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、
生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする管理装置。

【請求項１９】　前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、
所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、
端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と

同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であることを特徴とする請求項１８記載の管理装置。

【請求項２０】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項１９記載の管理装置。

【請求項２１】　複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、

無効化すべき端末装置を特定するためのものとして１以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、

端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、

前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、

前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする暗号通信装置。

【請求項２２】　前記無効化端末特定情報取得手段により取得される前記無効化端末特定情報は、

所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、

端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、

前記判定手段は、

前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、

当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することを特徴とする請求項２１記載の暗号通信装置。

【請求項２３】　複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、

前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする情報生成方法。

【請求項２４】　前記生成ステップは、前記所定ビット数をＮとすると、前記端末識別子取得ステップにより取得された端末識別子のうち最上位ビットからＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値を１以上特定し、各Ｘの値について、Ｘなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからＸビットの部分のビット列の値を示す値情報とを対応付けて、対応付けた有効上位桁情報と値情報との全ての組を構成要素とする前記無効化端末特定情報を生成することを特徴とする請求項２３記載の情報生成方法。

【請求項２５】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項２４記載の情報生成方法。

【請求項２６】　前記生成ステップは、前記所定ビット数をＮとすると、

前記端末識別子取得ステップにより取得されたいずれかの端末識別子の最下位ビットのみ反転したＮビットのビット列であって、当該端末識別子取得ステップにより取得された他のいずれかの端末識別子とも値が同一でないという条件を満たすビット列を、例外情報として定めるとともに、当該ビット列を端末識別子とみなし、

前記端末識別子取得ステップにより取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットか

らＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値で、かつ、Ｎ未満であるＸの値を、１以上特定し、
特定した各Ｘの値について、当該Ｘの値と、当該条件に係る２の（Ｎ－Ｘ）乗個の端末識別子の最上位ビットからＸビットの部分のビット列の値と対応付けて、対応付けた値の全ての組と前記例外情報とを構成要素とする前記無効化端末特定情報を生成することを特徴とする請求項２３記載の情報生成方法。

【請求項２７】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、
前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すことを特徴とする請求項２６記載の情報生成方法。

【請求項２８】　複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成処理をコンピュータに実行させるためのプログラムであって、
前記情報生成処理は、
前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、
前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とするプログラム。

【請求項２９】　複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成処理をコンピュータに実行させるためのプログラムを記録した記録媒体であって、
前記情報生成処理は、
前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、
前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする記録媒体。

【請求項３０】　端末装置から送信される端末識別子に基づいて当該端末装置が無効化すべき端末装置であるか否かを判定する判定処理をコンピュータに実行させるためのプログラムであって、
前記判定処理は、
端末装置から送信される所定ビット数の端末識別子を受信する端末識別子受信ステップと、
前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、無効化すべき１以上の端末装置の各端末識別子を特定する無効化端末特定情報を取得する無効化端末特定情報取得ステップと、
前記端末識別子受信ステップにより受信された端末識別子が、前記無効化端末特定情報により特定される何れかの端末識別子と一致するか否かを判定する判定ステップを含むことを特徴とするプログラム。

【請求項３１】　端末装置から送信される端末識別子に基づいて当該端末装置が無効化すべき端末装置であるか否かを判定する判定処理をコンピュータに実行させるためのプログラムを記録した記録媒体であって、
前記判定処理は、
端末装置から送信される所定ビット数の端末識別子を受信する端末識別子受信ステップと、
前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、無効化すべき１以上の端末装置の各端末識別子を特定する無効化端末特定情報を取得する無効化端末特定情報取得ステップと、
前記端末識別子受信ステップにより受信された端末識別子が、前記無効化端末特定情報により特定される何れかの端末識別子と一致するか否かを判定する判定ステップを含むことを特徴とする記録媒体。

【請求項３２】　無効化端末特定データを記録したコンピュータ読み取り可能な記録媒体であって、
前記無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、
前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、
当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする記録媒体。

【請求項３３】　前記端末識別子特定フィールドは、
所定ビット数のビット列中の一部分の値を示す値情報を記録した値情報フィールドと、
前記ビット列中における前記部分のビット位置を特定するための位置情報を記録した位置情報フィールドとを対応付けてなる組を１組以上含んで構成され、
前記無効化端末特定データは、
端末識別子中の部分的なビット列であって前記各位置情報フィールド内の各位置情報により特定されるビット位

置に所在する部分的なビット列の値が、当該位置情報が記録された位置情報フィールドに対応する値情報フィールドに記録された値情報で示される値と、同一である全ての端末識別子それぞれを、無効化すべき各端末装置の端末識別子として特定するデータであることを特徴とする請求項３２記載の記録媒体。

【請求項３４】　前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、

前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すことを特徴とする請求項３３記載の記録媒体。

【請求項３５】　複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、

前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、

当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする無効化端末特定データ。

【請求項３６】　暗号通信装置と、当該暗号通信装置に所定ビット数の鍵識別子を送信する端末装置と、無効化すべき１以上の各鍵識別子を特定する無効化鍵識別子特定情報を生成する管理装置とを備える暗号通信システムであって、

前記管理装置は、

前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての鍵識別子を包括的に表現するデータ形式を用いて、前記無効化鍵識別子特定情報を生成する無効化鍵識別子特定情報生成手段と、

生成された前記無効化鍵識別子特定情報を出力する出力手段とを有し、

前記暗号通信装置は、

前記管理装置により出力された前記無効化鍵識別子特定情報を取得する無効化鍵識別子特定情報取得手段と、

端末装置から鍵識別子を受信する鍵識別子受信手段と、

前記鍵識別子受信手段により受信された鍵識別子が、前記無効化鍵識別子特定情報により特定される何れかの鍵識別子と一致するか否かを判定する判定手段と、

前記受信された鍵識別子が前記無効化鍵識別子特定情報により特定される何れの鍵識別子とも一致しないと前記判定手段により判定された場合に限って、当該鍵識別子を送信した端末装置との間で、当該鍵識別子について固有な暗号化を施すことにより所定の通信を行う通信手段とを有することを特徴とする暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号通信システムに関し、特に、複数の端末装置のうち一部の端末装置からの要求には応えず、他の端末装置からの要求を受け付けてその端末装置に暗号化データを送信する暗号通信装置を含む暗号通信システムに関する。

【０００２】

【従来の技術】近年、インターネット関連技術の進展を背景として、インターネットを利用した電子商取引のシステム等が盛んに開発されている。電子商取引等におけるデータ通信では暗号技術が用いられる。例えば、通信相手の認証のためにしばしば公開鍵暗号系の暗号通信方式が用いられ、データを安全に配信するためにしばしば秘密鍵暗号系の暗号通信方式が用いられる。公開鍵暗号系及び秘密鍵暗号系の暗号技術については、文献「現代暗号理論」（池野信一、小山謙二、電子通信学会、1986年）に詳しく説明されている。

【０００３】公開鍵暗号系の暗号通信方式においては、一般に、公開鍵とそれを保有する人や物等の対応関係を証明すべく認証局と呼ばれる機関が発行した公開鍵証明書が、公開鍵に付加されて送信される。公開鍵証明書は基本的に秘密に扱われる必要のない公開情報である。なお、公開鍵と対になる秘密鍵は秘密に管理される必要がある。

【０００４】通常、公開鍵証明書は有効期間を持つが、公開鍵と対になる秘密鍵が事故や事件により暴露された場合又は暴露された疑いがある場合は、有効期間内であっても、その公開鍵証明書を無効化する必要がある。公開鍵証明書を無効化する方法として、文献「ディジタル署名と暗号技術」（山田慎一郎訳、株式会社ピアソン・エデュケーション、189頁～196頁、1997年）には、証明書廃棄リスト（ＣＲＬ：Certificate Revocation List）を公開する方法が示されている。このＣＲＬには、無効化すべき全ての公開鍵証明書のシリアル番号が記載されており、ＣＲＬを利用して、ＣＲＬに記載されているシリアル番号の付いた公開鍵証明書を、無効とし使用できなくなるような機構が構築できる。

【０００５】ところで、著作権保護その他の目的から暗号化されている映画等のデジタルコンテンツを適切に利用すべきことが要求されるデジタルコンテンツ受信再生用の多数の端末装置に対し、その要求に応じて配信装置がデジタルコンテンツの復号用の鍵（以下、「コンテンツ鍵」という。）を配信するような配信サービスについて考えた場合、著作権保護等に鑑みれば、そのコンテンツ鍵の配信は、適切な端末装置に対してのみ行われるべきである。

【０００６】この配信サービスにおいて、端末装置は装置固有の秘密鍵を有し、鍵を配信する側の配信装置は、端末装置からコンテンツ鍵の配信要求とともに端末装置固有の端末識別子（端末ＩＤ）の通知を受けて、コンテンツ鍵に、その端末装置固有の秘密鍵でのみ復号可能な暗号化を施してその端末装置に送信するような配信方式等が用いられると考えられる。

【０００７】この場合に、ある一部のメーカーが製造した端末装置における秘密鍵の実装方法に問題があることが判明した後には、そのメーカーの一群の端末装置に対してはコンテンツの鍵の配信を行わないようにする必要がある。また、端末装置におけるデジタルコンテンツのコピーを防止する等の機構について、ある一部のメーカーが製造した端末装置におけるその機構を無力化する方法が暴露された後には、そのメーカーの一群の端末装置に対してはコンテンツ鍵の配信を行わないようにする必要がある。

【０００８】即ち、不正な状態となった端末装置に対してのコンテンツ鍵の配信を停止する必要がある。この必要性に応える方法として、配信サービスにおいて、配信装置は、端末装置からコンテンツ鍵の配信要求とともに端末ＩＤを受け取ることとし、上述の公開鍵証明書のシリアル番号の代わりに無効化すべき全ての端末装置についての端末ＩＤを記載しておくこととした変形版のＣＲＬ（以下、「ＴＲＬ」（無効化端末リスト、Terminal Revocation List）という。）を用いることとし、受け取った端末ＩＤがＴＲＬに記載されていれば、その配信要求に応じず、記載されていない場合にのみ配信要求に応じて鍵を配信するというような方法が考えられる。

【０００９】

【発明が解決しようとする課題】しかしながら、上述の方法では、無効化すべき端末装置が多数の場合に、その全ての端末装置の端末ＩＤを記載するのでＴＲＬのデータサイズが膨大になる。仮に、配信サービスの対象とする端末装置を、約４０億台とし、端末ＩＤを４バイト以上の固定長データとし、その端末装置のうちの１％を無効化する必要があると想定した場合には、ＴＲＬは１６０メガバイト以上のデータサイズになる。

【００１０】このため、配信サービスにおいて、多数の端末装置に対応するために、コンテンツ鍵を配信する側の配信装置を各地域等に分散して多数設けておき、１つの管理装置でＴＲＬを生成してそのＴＲＬにデジタル署名等を含め、公衆通信網等を通じて各配信装置に送信し、各配信装置ではそのＴＲＬに基づいて端末装置への配信可否を判定するような運用形態を想定した場合、通信データ量が多く、また、各配信装置が保持すべきデータ量も多くなることから、この配信サービスは実用に耐えないものとなるおそれがある。

【００１１】例えば、無効化すべき端末装置が増加する毎にＴＲＬの送信を行うこととしたならば、通信データ量の多さにより、通信渋滞を招いてしまう。また、配信装置が端末装置から端末ＩＤを伴い配信要求を受けた時点で管理装置に最新のＴＲＬを要求して、ＴＲＬを受け取ってからＴＲＬに基づき端末ＩＤの照合を行うこととしたならば、配信装置がＴＲＬの受信に多くの時間を要することにより、端末装置からの要求への応答が遅れてしまう。

【００１２】そこで、本発明は、かかる問題に鑑みてなされたものであり、ＴＲＬを用いて一部の無効化すべき端末装置を除いた適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う暗号通信システムであって、ＴＲＬのデータサイズを抑えて実用性を高めた暗号通信システムを、提供することを目的とする。

【００１３】また、本発明は、上述の暗号通信システムの構築に資する各種技術を提供することをも目的とする。

【００１４】

【課題を解決するための手段】上記課題を達成するために、本発明に係る暗号通信システムは、暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして１以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする。

【００１５】ここで、暗号通信装置は、例えば実施の形態１～３で示すようなコンテンツ鍵配信装置であり、所定の通信とは例えば暗号化コンテンツ鍵の送信であり、無効化端末特定情報は例えば実施の形態１～３において示すＴＲＬである。本発明により、あるビット列を含む全ての端末ＩＤを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、ＴＲＬのデータ量を比較的小さく抑えることができるようになり、この結果、一部の無効化すべき端末装置を除い

た適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う実用的な暗号通信システムが実現される。

【００１６】また、本発明に係る管理装置は、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき１以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする。

【００１７】また、本発明に係る暗号通信装置は、複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、無効化すべき端末装置を特定するためのものとして１以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする。

【００１８】また、本発明に係る情報生成方法は、複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする。

【００１９】

【発明の実施の形態】以下、本発明をコンテンツの著作権保護等に配慮したシステムに応用した一実施形態であるコンテンツ鍵配信システムについて、図面を用いて説明する。

＜実施の形態１＞

＜システム構成＞図１は、本発明の実施の形態１に係るコンテンツ鍵配信システムの構成図である。

【００２０】コンテンツ鍵配信システム１００は、コンテンツを再生する複数のコンテンツ再生装置１３０と、暗号化されたコンテンツ鍵（以下、「暗号化コンテンツ鍵」という。）を各コンテンツ再生装置の要求に応じて配信するコンテンツ鍵配信装置１２０と、コンテンツ鍵配信装置１２０に対して暗号化コンテンツ鍵の配信可否の判断材料となる情報である無効化端末リスト（ＴＲＬ）を送信する管理装置１１０を含んで構成される。なお、コンテンツ鍵配信システム１００においてコンテンツ鍵配信装置１２０は、１台又は複数台備えられる。

【００２１】ここで、コンテンツ再生装置１３０ａ、１３０ｂ等は、例えば各家屋に設置され、通信路又は記録媒体等を経由して暗号化されたコンテンツを取得し、そのコンテンツをコンテンツ鍵を用いて復号して再生する機能を有する装置である。著作権保護等に配慮したシステムにおいては、コンテンツは暗号化され流通の対象とされることを想定している。このため、コンテンツ再生装置は、暗号化コンテンツ鍵をコンテンツ鍵配信装置１２０から受信し復号することによりコンテンツ鍵を得なければ、その暗号化されたコンテンツを、復号できず、そのため再生できない。

【００２２】コンテンツ再生装置１３０（以下、「端末」ともいう。）は各々、ＣＰＵ、メモリ、ハードディスク、外部との通信機構等を備えておりディスプレイ装置やスピーカ等を通じて、映画等のコンテンツをユーザに視聴可能なように再生するコンテンツ再生処理を行う装置であって、機能的には端末ＩＤ記憶部１３１、復号鍵記憶部１３２、暗号化コンテンツ格納部１３３、要求送出部１３４、暗号化コンテンツ鍵受信部１３５、復号部１３６及び再生部１３７を有する。

【００２３】端末ＩＤ記憶部１３１は、各端末を識別するための端末ＩＤを記憶しているＲＯＭ（read only memory）等の一記憶領域である。例えば、コンテンツ鍵配信システム１００において１６台の端末が用いられ得る場合には、１６台を識別可能な４ビット以上のビット列で端末ＩＤは構成され、例えば、５０億台の端末を想定する場合には端末ＩＤは３２ビットを超えるビット列となる。なお、実施の形態１においては、説明の便宜上、１６台の端末を想定して、端末ＩＤを４ビットとした例を主に用いて説明する。

【００２４】復号鍵記憶部１３２は、暗号化コンテンツ鍵の復号用に用いられる復号鍵を記憶しているＲＯＭ等

の一記憶領域である。この復号鍵は、端末毎に固有の値を有する秘密鍵であり、例えば１２８ビットで構成される。暗号化コンテンツ格納部１３３は、暗号化されたコンテンツを格納するハードディスク等の記録媒体の一領域である。なお、端末は暗号化されたコンテンツを受信等により外部から取得して暗号化コンテンツ格納部１３３に格納する機能を有する。

【００２５】要求送出部１３４は、端末ＩＤ記憶部１３１に記憶されている端末ＩＤを含む送信要求情報を公衆網等の通信路１０１を通じてコンテンツ鍵配信装置１２０に送信する機能を有する。暗号化コンテンツ鍵受信部１３５は、コンテンツ鍵配信装置１２０から暗号化コンテンツ鍵が送信された場合にその暗号化コンテンツ鍵を受信する機能を有する。

【００２６】復号部１３６は、暗号化コンテンツ鍵受信部１３５により受信された暗号化コンテンツ鍵を受け取ると復号鍵記憶部１３２に記憶されている復号鍵を用いてその暗号化コンテンツ鍵を復号し、復号の結果として得られるコンテンツ鍵を再生部１３７に送出する機能を有する。また、再生部１３７は、暗号化コンテンツ格納部１３３に格納されている暗号化されているコンテンツを、復号部１３６から伝えられたコンテンツ鍵を用いて復号して再生する機能を有する。この再生部１３７によりコンテンツが再生されると、ユーザはコンテンツを視聴できる。

【００２７】なお、要求送出部１３４、暗号化コンテンツ鍵受信部１３５、復号部１３６及び再生部１３７の行う機能の一部は、メモリに格納された制御プログラムがＣＰＵに実行されることにより実現される。管理装置１１０は、例えばコンテンツの著作権等の保護に関する業務を行う機関に設置されるコンピュータ等であり、各端末１３０のうち、内部に記憶されている復号鍵が暴露される等により著作権等の保護が図れない事態に陥っている全ての端末、即ち暗号化コンテンツ鍵の配信先にすべきでない全ての端末を、特定するための情報を主たる内容とするＴＲＬを生成してコンテンツ鍵配信装置１２０に送信するＴＲＬ生成送信処理を行う装置である。以下、暗号化コンテンツ鍵の配信先にすべきでない端末を無効化端末という。

【００２８】この管理装置１１０は、図１に示すように、無効化端末ＩＤ群取得部１１１、ＴＲＬ生成部１１２、ＴＲＬ送信部１１３を備える。ここで、無効化端末ＩＤ群取得部１１１は、全ての無効化端末についての端末ＩＤを特定する情報を取得し、取得した各端末ＩＤをＴＲＬ生成部１１２に与える機能を有する。

【００２９】ＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１から与えられた各端末ＩＤに基づいて無効化端末を特定する情報を主たる内容とするＴＲＬを生成し、ＴＲＬ送信部１１３に伝える機能を有する。なお、このＴＲＬの生成については、後に詳しく説明する。また、ＴＲＬ送信部１１３は、ＴＲＬ生成部１１２から伝えられたＴＲＬを通信路を通じてコンテンツ鍵配信装置１２０に対して送信する機能を有する。

【００３０】管理装置１１０が行うＴＲＬ生成送信処理の手順については後に説明する。なお、この管理装置１１０は、定期的或いはＴＲＬに含めるべき無効化端末の情報が変化した時等に、ＴＲＬをコンテンツ鍵配信装置１２０に送信するように運用されることが想定される。

コンテンツ鍵配信装置１２０は、各端末からの暗号化コンテンツ鍵の送信要求を受けるとその端末が無効化端末でない場合に限りその端末に暗号化コンテンツ鍵を送信することを内容とするコンテンツ鍵配信処理を行うコンピュータであり、機能的には、ＴＲＬ格納部１２１、ＴＲＬ受信部１２２、コンテンツ鍵記憶部１２３、暗号化鍵群記憶部１２４、送信要求受付部１２５、照合部１２６、暗号化部１２７及び暗号化コンテンツ鍵送信部１２８を有する。

【００３１】ここで、ＴＲＬ格納部１２１は、ＴＲＬを格納するためのハードディスク等の記録媒体の一領域である。ＴＲＬ受信部１２２は、管理装置１１０から送信されるＴＲＬを受信してＴＲＬ格納部１２１に格納する機能を有する。コンテンツ鍵記憶部１２３は、コンテンツ鍵を記憶しているメモリ等の一記憶領域である。

【００３２】暗号化鍵群記憶部１２４は、各端末について、その復号鍵に呼応する暗号化鍵とその端末の端末ＩＤと対応付けて、予め格納しているハードディスク等の一領域である。送信要求受付部１２５は、公衆網等を通じて各端末から送られる送信要求を受け付けて、送信要求に含まれる端末ＩＤを照合部１２６に伝える機能を有する。

【００３３】照合部１２６は、送信要求受付部１２５から伝えられた端末ＩＤが、ＴＲＬにより特定される無効化端末のいずれかと一致するか否かを照合することにより送信要求元の端末が無効化端末であるか否かを判定し、無効化端末であると判定した場合にはエラーメッセージを送信元に返すべき旨の指示を暗号化コンテンツ鍵送信部１２８に伝え、無効化端末でないと判定した場合には送信要求受付部１２５から伝えられた端末ＩＤを暗号化部１２７に伝える機能を有する。

【００３４】暗号化部１２７は、照合部１２６から端末ＩＤを伝えられた場合には、暗号化鍵群記憶部１２４においてその端末ＩＤと対応付けられている暗号化鍵を用いて、コンテンツ鍵記憶部１２３に格納されているコンテンツ鍵を暗号化することにより、暗号化コンテンツ鍵を生成して暗号化コンテンツ鍵送信部１２８に送出する機能を有する。

【００３５】また、暗号化コンテンツ鍵送信部１２８は、照合部１２６からエラーメッセージを送信元に返すべき旨の指示を伝えられた場合には、送信要求を発した端末に対してエラーメッセージを送信し、暗号化部１２

７から暗号化コンテンツ鍵を伝えられた場合には、送信要求を発した端末に対してその暗号化コンテンツ鍵を送信する機能を有する。

【００３６】＜端末ＩＤ／復号鍵／暗号化鍵＞図２は、各端末が記憶している端末ＩＤと復号鍵とを示す図である。コンテンツ鍵配信システム１００が、１６台の端末を含み、端末ＩＤは４ビットである場合において、同図に示すように、例えば端末０は「００００」という端末ＩＤと復号鍵ＤＫ０を保持し、端末１は「０００１」という端末ＩＤと復号鍵ＤＫ１を保持し、端末１５は「１１１１」という端末ＩＤと復号鍵ＤＫ１５を保持している。なお、復号鍵ＤＫ０、ＤＫ１、・・・、ＤＫ１５はいずれも、相互に値が一致しないビット列である。また、各端末は、復号鍵を耐タンパ技術等によって秘密状態で保護する。

【００３７】図３は、各端末が保持する端末ＩＤの値の決定方法を示す概念図である。例えば著作権等の保護に関する業務を行う機関によって、各メーカーの製造する各端末への端末ＩＤの割り当てが定められ、メーカーは端末の製造段階において、その割り当てに従って各端末にその割り当てられた端末ＩＤを記憶したＲＯＭ等をセットする。

【００３８】図３中の円をノードといい、円と円を繋ぐ直線をパスと表現すると、図３では、１６台の各端末を最下位レイヤの各々のノード１２と対応付けるように２分木の木構造を定め、あるノードから下位のレイヤのノードへの２つのパスそれぞれに「０」と「１」とのいずれかの値を付している。各端末の端末ＩＤは、最上位レイヤのノード１１からその端末に対応する最下位レイヤのノード１２とを結ぶ全てのパスに付された「０」又は「１」の値を、上位のレイヤから下位のレイヤの方向に連結して得られたビット列で表される。従って、図２で示したように各端末について端末ＩＤが定められる。

【００３９】図４は、コンテンツ鍵配信装置１２０の暗号化鍵群記憶部１２４に記憶されるデータの内容例を示した図である。暗号化鍵群記憶部１２４には、同図に示すように、全ての端末に対する端末ＩＤと暗号化鍵とが対応付けられて格納されている。例えば、「００００」という端末ＩＤには暗号化鍵ＥＫ０が対応付けられており、この暗号化鍵ＥＫ０は端末０に保持されている復号鍵ＤＫ０と呼応する鍵である。従って、暗号化鍵ＥＫ０を用いて暗号化されたデータは復号鍵ＤＫ０を用いて復号することが可能となる。

【００４０】なお、暗号化鍵ＥＫｉとそれに呼応する復号鍵ＤＫｉは、コンテンツ鍵を暗号化するための暗号化アルゴリズムに秘密鍵暗号系を用いるのであればＥＫｉとＤＫｉとは一致し、公開鍵暗号系を用いるのであればＥＫｉとＤＫｉとは一致はしないが対となるものである。

＜システム動作＞以下、コンテンツ鍵配信システム１００のシステム動作の概要について説明する。

【００４１】＜管理装置の動作＞図５は、管理装置１１０が行うＴＲＬ生成送信処理を示すフローチャートである。管理装置１１０のＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１より無効化端末についての端末ＩＤ群を取得し（ステップＳ２１）、ＴＲＬにおける無効化端末を特定する情報部分（以下、「端末ＩＤ関連情報」という。）の内容を算定するＴＲＬ用データ生成処理を行う（ステップＳ２２）。ＴＲＬ用データ生成処理の詳細については後述する。

【００４２】ＴＲＬ用データ生成処理の後、ＴＲＬ生成部１１２は、生成した端末ＩＤ関連情報を含めたＴＲＬを構築し（ステップＳ２３）、そのＴＲＬをＴＲＬ送信部１１３に伝え、これを受けてＴＲＬ送信部１１３はそのＴＲＬを通信路を通じてコンテンツ鍵配信装置１２０に送信する（ステップＳ２４）。

＜コンテンツ再生装置の動作＞図６は、コンテンツ再生装置１３０が行うコンテンツ再生処理を示すフローチャートである。

【００４３】コンテンツ再生装置１３０（端末）は、例えばユーザのコンテンツ再生を指示する操作を受けたとき等に、コンテンツ再生処理を行う。まず、端末の要求送出部１３４が、端末ＩＤ記憶部１３１に記憶されている自端末固有の端末ＩＤを含めたデータで構成される送信要求を通信路を通じてコンテンツ鍵配信装置１２０に送信することにより、暗号化コンテンツ鍵の送信を要求する（ステップＳ３１）。なお、この送信要求に応答して、コンテンツ鍵配信装置１２０からは暗号化コンテンツ鍵、又はエラーメッセージが送られることになる。

【００４４】送信要求の後に、暗号化コンテンツ鍵受信部１３５は、暗号化コンテンツ鍵の受信に成功したかを判定し（ステップS.３２）、暗号化コンテンツ鍵が正常に受信された場合に限り、その暗号化コンテンツ鍵を復号部１３６に伝える。これを受けて復号部１３６は復号鍵記憶部１３２に保持されている復号鍵を用いて暗号化コンテンツ鍵を復号して、その復号の結果として得られるコンテンツ鍵を再生部１３７に伝える（ステップＳ３３）。

【００４５】コンテンツ鍵を伝えられると再生部１３７は、暗号化コンテンツ格納部１３３に格納されている暗号化されたコンテンツをそのコンテンツ鍵を用いて復号しつつ再生する（ステップＳ３４）。この再生により、例えばディスプレイ装置やスピーカを通じて映像、音声等が出力され、ユーザはコンテンツの視聴が可能になる。

【００４６】＜コンテンツ鍵配信装置の動作＞図７は、コンテンツ鍵配信装置１２０が行うコンテンツ鍵配信処理を示すフローチャートである。コンテンツ鍵配信装置１２０は、ＴＲＬを、コンテンツ鍵配信処理を行う前に少なくとも１度はＴＲＬ受信部１２２により受信してＴ

ＲＬ格納部１２１に格納しており、コンテンツ再生装置１３０から送信要求が送られる度にコンテンツ鍵配信処理を行う。

【００４７】コンテンツ再生装置１３０（端末）から送信要求が送られると、送信要求受付部１２５は送信要求を受信しその送信要求に含まれる端末ＩＤを照合部１２６に伝える（ステップＳ４１）。照合部１２６は、端末ＩＤが伝えられると、ＴＲＬを参照してその端末ＩＤが無効化端末の端末ＩＤであるか否かを判定するＴＲＬ照合処理を行う（ステップＳ４２）。なお、ＴＲＬ照合処理の詳細については後述する。

【００４８】ＴＲＬ照合処理の結果として、送信要求に係る端末ＩＤが、無効化端末の端末ＩＤであると判定した場合には（ステップＳ４３）、照合部１２６はエラーメッセージを送信要求の送信元の端末に返すべき旨の指示を暗号化コンテンツ鍵送信部１２８に伝えて、これに応じて暗号化コンテンツ鍵送信部１２８がエラーメッセージをその端末に送信するといったエラー処理を行い（ステップＳ４７）、コンテンツ鍵配信処理を終了する。

【００４９】ステップＳ４３においてＴＲＬ照合処理の結果として、送信要求に係る端末ＩＤが、無効化端末の端末ＩＤではないと判定した場合には、照合部１２６は、送信要求に係る端末ＩＤを暗号化部１２７に伝え、これを受けて暗号化部１２７は、その端末ＩＤに対応する暗号化鍵を暗号化鍵群記憶部１２４から取り出してその暗号化鍵を用いて、コンテンツ鍵記憶部１２３に記憶されているコンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、その暗号化コンテンツ鍵を暗号化コンテンツ鍵送信部１２８に伝える（ステップＳ４５）。

【００５０】暗号化コンテンツ鍵を伝えられると、暗号化コンテンツ鍵送信部１２８はその暗号化コンテンツ鍵を送信要求を発した端末に送信し（ステップＳ４６）、これでコンテンツ鍵配信処理は終了する。

＜ＴＲＬの構成＞図８は、実施の形態１におけるＴＲＬのデータ構成を示す図である。

【００５１】なお、同図中のビットサイズ例は端末が１６台の場合を想定しているが、括弧内には、参考のため実用的な例として、端末数が数億台以上である場合に対応したビットサイズの例を示している。以下、端末が１６台の場合についてのビットサイズ例を用いて説明する。同図に示すように、ＴＲＬは、８ビットのバージョン情報２１０と、端末ＩＤ関連情報２２０と、６４ビットの署名情報２３０とから構成される。

【００５２】バージョン情報２１０は、ＴＲＬのバージョン番号を示す情報であり、例えば内容の異なるＴＲＬが新たに生成される毎に、そのバージョン番号が変えられる。端末ＩＤ関連情報２２０は、グループ情報２２１と個別情報２２５とから構成される。

【００５３】グループ情報２２１は、ＩＤ２２３とマスクデータ２２４との組の１個又は複数個を含み、その個数を示すエントリ数２２２を含む。その組の数がＭ個であれば、エントリ数２２２の示す値はＭとなる。ここで、マスクデータ２２４は、これを構成する４ビットのビット列のうち上位Ｘビットを「１」にし残りの下位ビットがあればその下位ビット全てを「０」とした形式のデータであり、これによりＸが表現される。

【００５４】また、Ｘを表すマスクデータ２２４と組をなすＩＤ２２３は、これを構成する４ビットのビット列のうち上位からＸビット分の内容のみが有用であり、その他の値は例えば「０」とした形式のデータとなる。このＩＤ２２３とマスクデータ２２４との組により、マスクデータ２２４で表される上位ＸビットがＩＤ２２３の値と一致する全ての端末ＩＤを、即ち２の（４－Ｘ）乗個の無効化端末の端末ＩＤを示す。

【００５５】従って、グループ情報２２１は、複数の無効化端末の端末ＩＤを包括的に表現する１又は複数の組から成る。個別情報２２５は、１又は複数個のＩＤ２２７を含み、その個数を示すエントリ数２２６を含む。ＩＤ２２７の個数がＮ個であれば、エントリ数２２６の示す値はＮとなる。

【００５６】このＩＤ２２７は、無効化端末の端末ＩＤを示す。従って、個別情報２２５は、個別に無効化端末の端末ＩＤを表現する１又は複数の情報から成る。署名情報２３０は、バージョン情報２１０及び端末ＩＤ関連情報２２０の全体を反映して作成されるいわゆるデジタル署名である。図９は、ＴＲＬの内容例を示す図である。

【００５７】同図では、グループ情報として、ＩＤ２２３がビット列「１１００」であってマスクデータ２２４がビット列「１１００」である組とＩＤ２２３がビット列「０１１０」であってマスクデータ２２４がビット列「１１１０」である組とを有し、個別情報として、ＩＤ２２７がビット列「０００１」である情報を含むＴＲＬを例示している。

【００５８】この「１１００」なるマスクデータと「１１００」なるＩＤとの組により、「１１００」、「１１０１」、「１１１０」及び「１１１１」という４個の無効化端末の端末ＩＤが表され、また、「１１１０」なるマスクデータと「０１１０」なるＩＤとの組により、「０１１０」及び「０１１１」という２個の無効化端末の端末ＩＤが表される。

【００５９】従って、図９に示すＴＲＬは、グループ情報で６個と個別情報で１個の合計７個の無効化端末の端末ＩＤを示している。

＜ＴＲＬ用データ生成処理＞図１０は、実施の形態１における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。なお、同図では、端末ＩＤをＮビットと汎用的に表現しているが、ここでは４ビットであるもの

として説明する。

【００６０】管理装置１１０においてＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１より無効化端末についての端末ＩＤ群を取得した後にＴＲＬ用データ生成処理を行う（図５参照）。まず、ＴＲＬ生成部１１２は、取得した端末ＩＤ群をメモリ等の記憶媒体の一領域である作業用ＩＤ領域に格納し（ステップＳ２０１）、メモリ等の記憶媒体の一領域である作業用ビット領域に１ビットのビットデータ「０」と「１」との２つを格納し（ステップＳ２０２）、変数Ｘに１を設定する（ステップＳ２０３）。

【００６１】続いて、ＴＲＬ生成部１１２は、作業用ビット領域中、未着目のＸビットのビットデータの１つに着目し（ステップＳ２０４）、作業用ＩＤ領域中に格納されている端末ＩＤのうち、上位Ｘビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする（ステップＳ２０５）。ステップＳ２０５の結果、カウント数が２の（４－Ｘ）乗となった場合には（ステップＳ２０６）、ＴＲＬ生成部１１２は、ステップＳ２０５におけるその条件を満たす端末ＩＤを作業用ＩＤ領域から削除し（ステップＳ２０７）、その条件を満たす端末ＩＤについて、上位Ｘビット分を「１」として他のビットを「０」とした４ビットのビット列をマスクデータとして、更に上位Ｘビット分を着目中のビットデータと同一にして他のビットを「０」とした４ビットのビド列をＩＤとして、そのマスクデータとＩＤとを対応付けてグループ情報としてメモリ等の記憶媒体の一領域に保存し（ステップＳ２０８）、ステップＳ２０９の判断を行う。

【００６２】また、ステップＳ２０５の結果、カウント数が０又は１であった場合には（ステップＳ２０６）、ＴＲＬ生成部１１２は、ステップＳ２０７及びステップＳ２０８をスキップしてステップＳ２０９の判断を行う。また、ステップＳ２０５の結果、カウント数が２の（４－Ｘ）乗、０及び１のいずれでもない場合には（ステップＳ２０６）、ＴＲＬ生成部１１２は、ステップＳ２０５におけるその条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「０」のものが２個以上存在すれば、着目中のビットデータの下位に１ビットの「０」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ２１０）、その条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「１」のものが２個以上存在すれば、着目中のビットデータの下位に１ビットの「１」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ２１１）、ステップＳ２０９の判断を行う。

【００６３】ステップＳ２０９では、ＴＲＬ生成部１１２は、未着目のＸビットのビットデータが存在するか否かを判定し、未着目のＸビットのビットデータが未だ存在すればステップＳ２０４に戻って次のビットデータに着目して処理を行い、未着目のＸビットのビットデータが存在しなければ変数Ｘを１増加し（ステップＳ２１２）、変数Ｘが４と等しいか否かを判定する（ステップＳ２１３）。

【００６４】ＴＲＬ生成部１１２は、ステップＳ２１３において変数Ｘが４と等しくないと判定した場合には、再びステップＳ２０４に戻って次のビットデータに着目して処理を行い、変数Ｘが４と等しいと判定した場合には、作業用ＩＤ領域に端末ＩＤが残っていればその全ての端末ＩＤを個別情報中のＩＤとしてメモリ等の記憶媒体の一領域に保存し（ステップＳ２１４）、これによりＴＲＬ用データ生成処理を終了する。

【００６５】なお、図５のステップＳ２３で示すＴＲＬの構築は、上述のＴＲＬ用データ生成処理によって記憶媒体の一領域に保存されたグループ情報及び個別情報に、それぞれエントリ数を付加して、更にバージョン情報及び署名情報を加えることによって実行される。従って、例えば、ＴＲＬ生成部１１２が無効化端末ＩＤ群取得部１１１から「０００１」、「０１１０」、「０１１１」、「１１００」、「１１０１」、「１１１０」及び「１１１１」の７個の端末ＩＤを取得した場合には、上述の手順により、図９に例示した内容のＴＲＬが生成されることになる。このＴＲＬは、図３において隣接した端末６及び端末７のグループと、端末１２～端末１５のグループと、更に端末１が無効化端末であることを表している。

【００６６】また、無効化端末が１台もない場合においては、ＴＲＬのグループ情報中のエントリ数は０となり、個別情報中のエントリ数も０となる。

＜ＴＲＬ照合処理＞図１１は、実施の形態１におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。

【００６７】コンテンツ鍵配信装置１２０の照合部１２６は、端末から送られた端末ＩＤを送信要求受付部１２５より得る度にこのＴＲＬ照合処理を行う。照合部１２６は、端末から送られた端末ＩＤと一致するＩＤ２２７が、ＴＲＬ格納部１２１に格納されているＴＲＬ中の個別情報２２５中に存在するか否かを判定し（ステップＳ２２１）、一致するＩＤ２２７が存在すれば端末から取得した端末ＩＤは無効化端末の端末ＩＤであると判定し（ステップＳ２２２）、ＴＲＬ照合処理を終了する。

【００６８】ステップＳ２２１において、端末から送られた端末ＩＤと一致するＩＤ２２７がＴＲＬの個別情報２２５中に含まれていないと判定した場合には、照合部１２６は、ＴＲＬのグループ情報中の１組のＩＤ２２３及びマスクデータ２２４で表されるいずれかの端末ＩＤと、端末から送られた端末ＩＤとが一致するかを検査する（ステップＳ２２３、Ｓ２２４）。

【００６９】即ち、照合部１２６は、端末から送られた

端末ＩＤとマスクデータ２２４とのビット毎の論理積を求めて（ステップＳ２２３）、求めた論理積がそのマスクデータ２２４と組をなすＩＤ２２３と一致するか否かを判定し（ステップＳ２２４）、一致すれば、端末から取得した端末ＩＤは無効化端末の端末ＩＤであると判定し（ステップＳ２２２）、ＴＲＬ照合処理を終了する。

【００７０】また、ステップＳ２２４において、一致しない場合には、照合部１２６はＴＲＬのグループ情報中の全てのＩＤ２２３とマスクデータ２２４との組についてステップＳ２２３及びステップＳ２２４の処理を行なったかを判定し（ステップＳ２２５）、全ての組についての処理済みでない場合にはステップＳ２２３及びステップＳ２２４の処理を再び行う。

【００７１】ステップＳ２２５において、全ての組について処理済みであると判定した場合には、照合部１２６は、端末から取得した端末ＩＤは無効化端末の端末ＩＤでないと判定し（ステップＳ２２６）、ＴＲＬ照合処理を終了する。以下、ＴＲＬ格納部１２１に格納されているＴＲＬは図９に例示した内容であることを前提として、図７及び図１１を用いて、端末１３から端末ＩＤ「１１０１」を含めた送信要求がコンテンツ鍵配信装置１２０に送られた場合を想定してコンテンツ鍵配信装置１２０の具体的動作について説明する。

【００７２】コンテンツ鍵配信装置１２０の送信要求受付部１２５は、端末１３から送られた端末ＩＤ「１１０１」を取得して照合部１２６に伝え（ステップＳ４１）、照合部１２６は、端末１３から送られた端末ＩＤ「１１０１」がＴＲＬの個別情報中にあるか否かを判定するが（ステップＳ２２１）、個別情報中には「０００１」というＩＤしか含まれていないため、端末ＩＤ「１１０１」とグループ情報中のマスクデータ「１１００」との論理積を求める（ステップＳ２２３）。

【００７３】このステップＳ２２３により求められる論理積は「１１００」となり、照合部１２６は、その求められたビット列「１１００」とＩＤ「１１００」とが一致するか否かを判定し（ステップＳ２２４）、一致するので、端末から取得した端末ＩＤは無効化端末のＩＤであると判定し（ステップＳ２２２）、この結果（ステップＳ４３）、エラーメッセージを送信すべき旨を暗号化コンテンツ鍵送信部１２８に伝え、これを受けて暗号化コンテンツ鍵送信部１２８がエラーメッセージを端末１３に送信する（ステップＳ４７）。

【００７４】次に、同じ前提の下で、復号鍵ＤＫ２を保持する端末２から端末ＩＤ「００１０」を含めた送信要求がコンテンツ鍵配信装置１２０に送られた場合を想定してコンテンツ鍵配信装置１２０の具体的動作について説明する。コンテンツ鍵配信装置１２０の送信要求受付部１２５は、端末２から送られた端末ＩＤ「００１０」を取得して照合部１２６に伝え（ステップＳ４１）、照合部１２６は、端末２から送られた端末ＩＤ「００１０」がＴＲＬの個別情報中にあるか否かを判定するが（ステップＳ２２１）、個別情報中には「０００１」というＩＤしか含まれていないため、端末ＩＤ「００１０」とグループ情報中のマスクデータ「１１００」との論理積を求める（ステップＳ２２３）。

【００７５】こうして求められる論理積は「０００」となり、照合部１２６は、その求められたビット列「０００」とＩＤ「１１００」とが一致するか否かを判定し（ステップＳ２２４）、一致しないので、次に、端末から送られた端末ＩＤ「００１０」と、グループ情報中のマスクデータ「１１１０」との論理積を求める（ステップＳ２２５、ステップＳ２２３）。

【００７６】こうして求められる論理積は「００１０」となり、照合部１２６は、その求められたビット列「００１０」とＩＤ「０１１０」とが一致するか否かを判定し（ステップＳ２２４）、一致せず、未処理のグループ情報中のマスクデータは既にないため（ステップＳ２２５）、端末から取得した端末ＩＤ「００１０」は無効化端末の端末ＩＤでないと判定し（ステップＳ２２６、Ｓ４３）、その端末ＩＤ「００１０」を暗号化部１２７に伝える。

【００７７】これを受けて暗号化部１２７は、暗号化鍵群記憶部１２４から「００１０」に対応する暗号化鍵ＥＫ２（図４参照）を抽出して用いることにより、コンテンツ鍵記憶部１２３に格納されているコンテンツ鍵を暗号化して（ステップＳ４５）、その結果として得られる暗号化コンテンツ鍵を暗号化コンテンツ鍵送信部１２８に伝える。

【００７８】暗号化コンテンツ鍵を伝えられると暗号化コンテンツ鍵送信部１２８は、その暗号化コンテンツ鍵を端末２に送信する（ステップＳ４６）。従って、この暗号化コンテンツ鍵を取得した端末２は、内部に保持する復号鍵ＤＫ２を用いて復号し、コンテンツ鍵を得ることができる。

＜実施の形態２＞以下、実施の形態２に係るコンテンツ鍵配信システムについて説明する。

【００７９】この実施の形態２に係るコンテンツ鍵配信システムは、実施の形態１で示したコンテンツ鍵配信システム１００と基本的に同様のシステム構成を有し、基本的に同様のシステム動作を行う。従って、各装置については図１等で付した符号を用いて示し、また、実施の形態１と同等の部分についての説明は省略する。但し、実施の形態２では、端末ＩＤのデータ構成を特別なものと定めており、また、ＴＲＬのデータ構造を実施の形態１におけるものとは異なったものにしている。このため、管理装置１１０は実施の形態１で示したＴＲＬ用データ生成処理とは異なるＴＲＬ用データ生成処理を行い、コンテンツ鍵配信装置１２０は実施の形態１で示したＴＲＬ照合処理とは異なるＴＲＬ照合処理を行う。

【００８０】＜端末ＩＤ＞図１２は、実施の形態２にお

ける端末ＩＤのデータ構成を示す図である。同図では、コンテンツ鍵配信システムにおける端末数として数億台以上に対応できるように端末ＩＤを１２８ビットのものとした構成例を示している。端末ＩＤは、３２ビットのメーカーＩＤフィールド３０１、３２ビットの製品ＩＤフィールド３０２、３２ビットの製品バージョンＩＤフィールド３０３、及び３２ビットのシリアル番号フィールド３０４で構成される。

【００８１】ここで、メーカーＩＤフィールド３０１には、コンテンツ再生装置を製造する各メーカーを識別するためのメーカーＩＤが格納される。製品ＩＤフィールド３０２には、メーカーＩＤで定まるメーカーにおける各製品を識別するための製品ＩＤが格納される。製品バージョンＩＤフィールド３０３には、製品ＩＤで定まる製品について形式変更等の都度変更されるバージョン番号等を示す製品バージョンＩＤが格納される。

【００８２】また、シリアル番号フィールド３０４には、製品個別に付されるシリアル番号が格納される。

＜ＴＲＬの構成＞図１３は、実施の形態２におけるＴＲＬのデータ構成を示す図である。同図では、端末数が数億台以上である場合に対応したＴＲＬのデータ構成例を示している。

【００８３】同図に示すように、ＴＲＬは、８ビットのバージョン情報３１０と、１２８ビットの発行者情報３２０と、１２８ビットの無効化端末数３３０と、端末ＩＤ関連情報３４０と、３２０ビットの署名情報３５０とから構成される。バージョン情報３１０は、ＴＲＬのバージョン番号を示す情報であり、例えば内容の異なるＴＲＬが新たに生成される毎に、そのバージョン番号が変えられる。

【００８４】発行者情報３２０は、管理装置等、ＴＲＬの発行元を示す情報である。無効化端末数３３０は、無効化端末の端末数である。端末ＩＤ関連情報３４０は、１２８ビットのＩＤ３４２と８ビットのマスク用ビット３４３との組の１個又は複数個を含み、その個数を示すエントリ数３４１を含む。その組の数がＮ個であれば、エントリ数３４１の示す値はＮとなる。

【００８５】ここで、マスク用ビット３４３は、１～１２８の値をとる。なお、このマスク用ビット３４３の値をＸとすると、１２８ビットのビット列のうち上位Ｘビットを「１」にし残りの下位ビットがあればその下位ビット全てを「０」とした形式のマスクデータを導出することができる。また、マスク用ビット３４３と組をなすＩＤ３４２は、これを構成する１２８ビットのビット列のうち上位からマスク用ビット３４３で示される値のビット桁数分の内容のみが有用であり、その他の値は例えば「０」とした形式のデータとなる。

【００８６】このＩＤ３４２とマスク用ビット３４３との組により、マスク用ビット３４３の値Ｘで表される上位ＸビットがＩＤ３４２の値と一致する全ての端末ＩＤを、即ち２の（１２８－Ｘ）乗個の無効化端末の端末ＩＤを示す。署名情報３５０は、バージョン情報３１０、発行者情報３２０、無効化端末数３３０及び端末ＩＤ関連情報３４０の全体を反映して作成されるいわゆるデジタル署名である。

【００８７】＜ＴＲＬ用データ生成処理＞図１４は、実施の形態２における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。ここでは、端末ＩＤをＮビットであるとして説明する。Ｎは、例えば１２８ビットである。

【００８８】管理装置１１０においてＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１より無効化端末についての端末ＩＤ群を取得した後にＴＲＬ用データ生成処理を行う（図５参照）。まず、ＴＲＬ生成部１１２は、取得した端末ＩＤ群をメモリ等の記憶媒体の一領域である作業用ＩＤ領域に格納し（ステップＳ３０１）、メモリ等の記憶媒体の一領域である作業用ビット領域に１ビットのビットデータ「０」と「１」との２つを格納し（ステップＳ３０２）、変数Ｘに１を設定する（ステップＳ３０３）。

【００８９】続いて、ＴＲＬ生成部１１２は、作業用ビット領域中、未着目のＸビットのビットデータの１つに着目し（ステップＳ３０４）、作業用ＩＤ領域中に格納されている端末ＩＤのうち、上位Ｘビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする（ステップＳ３０５）。ステップＳ３０５の結果、カウント数が２の（Ｎ－Ｘ）乗となった場合には（ステップＳ３０６）、ＴＲＬ生成部１１２は、ステップＳ３０５におけるその条件を満たす端末ＩＤを作業用ＩＤ領域から削除し（ステップＳ３０７）、その条件を満たす端末ＩＤについて、変数Ｘの値をマスク用ビットとして、更に上位Ｘビット分を着目中のビットデータと同一にして他のビットを「０」としたＮビットのビット列をＩＤとして、そのマスク用ビットとＩＤとを一組としてメモリ等の記憶媒体の一領域に保存し（ステップＳ３０８）、ステップＳ３０９の判断を行う。

【００９０】また、ステップＳ３０５の結果、カウント数が０又は１であった場合には（ステップＳ３０６）、ＴＲＬ生成部１１２は、ステップＳ３０７及びステップＳ３０８をスキップしてステップＳ３０９の判断を行う。また、ステップＳ３０５の結果、カウント数が２の（Ｎ－Ｘ）乗、０及び１のいずれでもない場合には（ステップＳ３０６）、ＴＲＬ生成部１１２は、ステップＳ３０５におけるその条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「０」のものが２個以上存在すれば、着目中のビットデータの下位に１ビットの「０」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ３１０）、その条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「１」のものが２個以

上存在すれば、着目中のビットデータの下位に１ビットの「１」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ３１１）、ステップＳ３０９の判断を行う。

【００９１】ステップＳ３０９では、ＴＲＬ生成部１１２は、未着目のＸビットのビットデータが存在するか否かを判定し、未着目のＸビットのビットデータが未だ存在すればステップＳ３０４に戻って次のビットデータに着目して処理を行い、未着目のＸビットのビットデータが存在しなければ変数Ｘを１増加し（ステップＳ３１２）、変数ＸがＮと等しいか否かを判定する（ステップＳ３１３）。

【００９２】ＴＲＬ生成部１１２は、ステップＳ３１３において変数ＸがＮと等しくないと判定した場合には、再びステップＳ３０４に戻って次のビットデータに着目して処理を行い、変数ＸがＮと等しいと判定した場合には、作業用ＩＤ領域に端末ＩＤが残っていればその全ての端末ＩＤについて、Ｎをマスク用ビットとしてその端末ＩＤをＩＤとして一組とし、メモリ等の記憶媒体の一領域に保存し（ステップＳ３１４）、これによりＴＲＬ用データ生成処理を終了する。

【００９３】なお、実施の形態２においては、図５のステップＳ２３で示すＴＲＬの構築は、上述のＴＲＬ用データ生成処理によって記憶媒体の一領域に保存されたＩＤとマスク用ビットとの１個又は複数個の組にエントリ数を付加し、更にバージョン、発行者情報、無効化端末数及び署名情報を加えることによって実行される。図１５は、ＴＲＬの内容例を示す図である。

【００９４】同図では、項目としては図１３に示したデータ項目を有し、端末ＩＤを４ビットのビット列とし、マスク用ビットは１～４までを表す２ビットのデータであることとしたＴＲＬの内容例を示している。なお、この図１５に例示する端末ＩＤ関連情報が表現する全ての無効化端末の端末ＩＤは、図９に例示する端末ＩＤ関連情報が表現する全ての無効化端末の端末ＩＤと同じである。

【００９５】＜ＴＲＬ照合処理＞図１６は、実施の形態２におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。コンテンツ鍵配信装置１２０の照合部１２６は、端末から送られた端末ＩＤを送信要求受付部１２５より得る度にこのＴＲＬ照合処理を行う。

【００９６】照合部１２６は、端末から送られた端末ＩＤと、ＴＲＬの端末ＩＤ関連情報中のＩＤとマスク用ビットとの組のいずれかで表される端末ＩＤとが一致するかを検査する（ステップＳ３２１～Ｓ３２４）。即ち、照合部１２６は、ＴＲＬ中の１つの未着目のマスク用ビットに着目し、そのマスク用ビットの値に応じたマスクデータを上述したように導出して（ステップＳ３２１）、端末から送られた端末ＩＤと、導出したマスクデータとのビット毎の論理積を求めて（ステップＳ３２２）、求めた論理積が着目中のマスク用ビット３４３と組をなすＩＤ３４２と一致するか否かを判定し（ステップＳ３２３）、一致すれば、端末から取得した端末ＩＤは無効化端末の端末ＩＤであると判定し（ステップＳ３２６）、ＴＲＬ照合処理を終了する。

【００９７】また、ステップＳ３２３において、一致しない場合には、照合部１２６はＴＲＬ中の全てのマスク用ビット３４３に着目してステップＳ３２１～Ｓ３２３の処理を行なったかを判定し（ステップＳ３２４）、全てのマスク用ビット３４３に着目して処理を行っていない場合にはステップＳ３２１に戻って未着目のマスク用ビットに着目して処理を行う。

【００９８】ステップＳ３２４において、全てのマスク用ビットについて処理済みであると判定した場合には、照合部１２６は、端末から取得した端末ＩＤは無効化端末の端末ＩＤでないと判定し（ステップＳ３２５）、ＴＲＬ照合処理を終了する。

＜考察＞実施の形態２に示したコンテンツ鍵配信システムにおいては、端末ＩＤが図１２に示したようなデータ構造であるため、あるメーカーが製造した特定バージョンの製品に実装されたあらゆるコンテンツ再生装置が無効化すべきものとなったような場合において、装置内に保持する端末ＩＤのシリアル番号フィールドの内容のみが異なる一群のコンテンツ再生装置の全てを、少ないデータ量で特定するＴＲＬを管理装置は生成してコンテンツ鍵配信装置に送信することができるようになる。

【００９９】そのＴＲＬは、例えば、マスク用ビット３４３の値を９６とし、ＩＤ３４２をそのメーカーのその製品のそのバージョンを特定し、かつ、シリアル番号については０としたビット列とした一組のみを端末ＩＤ関連情報として含むものとなる。

＜実施の形態３＞以下、実施の形態３に係るコンテンツ鍵配信システムについて説明する。

【０１００】この実施の形態３に係るコンテンツ鍵配信システムは、実施の形態１で示したコンテンツ鍵配信システム１００と基本的に同様のシステム構成を有し、基本的に同様のシステム動作を行う。従って、各装置については図１等で付した符号を用いて示し、また、実施の形態１と同等の部分についての説明は省略する。但し、実施の形態３では、端末ＩＤのデータ構造は実施の形態２で示したものを用い、またＴＲＬのデータ構造を、実施の形態１におけるものとは異なり、実施の形態２におけるＴＲＬに若干のデータ項目を追加したものにしている。このため、管理装置１１０は実施の形態２で示したＴＲＬ用データ生成処理とは若干異なるＴＲＬ用データ生成処理を行い、コンテンツ鍵配信装置１２０は実施の形態２で示したＴＲＬ照合処理とは若干異なるＴＲＬ照合処理を行う。

【０１０１】＜ＴＲＬの構成＞図１７は、実施の形態３におけるＴＲＬのデータ構成を示す図である。同図では、端末数が数億台以上である場合に対応したＴＲＬのデータ構成例を示している。同図に示すように、ＴＲＬは、８ビットのバージョン情報４１０と、１２８ビットの発行者情報４２０と、１２８ビットの無効化端末数４３０と、端末ＩＤ関連情報４４０と、３２０ビットの署名情報４５０とから構成される。

【０１０２】バージョン情報４１０、発行者情報４２０及び無効化端末数４３０は、実施の形態２で示したバージョン情報３１０、発行者情報３２０及び無効化端末数３３０と同一である。端末ＩＤ関連情報４４０は、１２８ビットのＩＤ４４２と８ビットのマスク用ビット４４３との組の１個又は複数個を含み、その個数を示すエントリ数４４１を含むところまでは、実施の形態２で示した端末ＩＤ関連情報３４０と同じであるが、更に１２８ビットの例外ＩＤ４４５を１個又は複数個含み、その個数を示す例外エントリ数４４４を含む。例外ＩＤの数がＭ個であれば、例外エントリ数４４４の示す値はＭとなる。

【０１０３】ここで、例外ＩＤ４４５は、無効化端末でない端末の端末ＩＤである。この端末ＩＤ関連情報４４０では、ＩＤ４４２とマスク用ビット４４３との組により複数の端末の端末ＩＤを包括的に表現するが、その組によって表現された端末ＩＤのうち無効化端末ＩＤでないものが、例外ＩＤ４４５によって示される。

【０１０４】従って端末ＩＤ関連情報４４０によれば、例えば仮に端末ＩＤが４ビットであり、端末として端末０から端末１５を想定した場合において、端末８～端末１５のうち端末１０を除く他のものは無効化端末である場合には、「１０００」というＩＤ４４２と値が１であるマスク用ビット４４３との組と「１０１０」という例外ＩＤとが端末ＩＤ関連情報の内容となる。

【０１０５】また、署名情報４５０は、バージョン情報４１０、発行者情報４２０、無効化端末数４３０及び端末ＩＤ関連情報４４０の全体を反映して作成されるいわゆるデジタル署名である。

＜ＴＲＬ用データ生成処理＞図１８は、実施の形態３における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。

【０１０６】ここでは、端末ＩＤをＮビットであるとして説明する。Ｎは、例えば１２８ビットである。管理装置１１０においてＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１より無効化端末についての端末ＩＤ群を取得した後にＴＲＬ用データ生成処理を行う（図５参照）。

【０１０７】まず、ＴＲＬ生成部１１２は、取得した端末ＩＤ群をメモリ等の記憶媒体の一領域である作業用ＩＤ領域に格納し（ステップＳ４０１）、各端末ＩＤのうち、最下位ビットのみが異なる端末ＩＤが作業用ＩＤ領域中に存在しないものについては、その最下位ビットのみが異なる端末ＩＤを生成して作業用ＩＤ領域に格納するとともにその生成した端末ＩＤを例外ＩＤとして保存する（ステップＳ４０２）。

【０１０８】続いて、ＴＲＬ生成部１１２は、メモリ等の記憶媒体の一領域である作業用ビット領域に１ビットのビットデータ「０」と「１」との２つを格納し（ステップＳ４０３）、変数Ｘに１を設定する（ステップＳ４０４）。ステップＳ４０４に続いて、ＴＲＬ生成部１１２は、作業用ビット領域中、未着目のＸビットのビットデータの１つに着目し（ステップＳ４０５）、作業用ＩＤ領域中に格納されている端末ＩＤのうち、上位Ｘビットが着目中のビットデータと一致するという条件を満たすものの数をカウントする（ステップＳ４０６）。

【０１０９】ステップＳ４０６の結果、カウント数が２の（Ｎ－Ｘ）乗となった場合には（ステップＳ４０７）、ＴＲＬ生成部１１２は、ステップＳ４０６におけるその条件を満たす端末ＩＤを作業用ＩＤ領域から削除し（ステップＳ４０８）、その条件を満たす端末ＩＤについて、変数Ｘの値をマスク用ビットとして、更に上位Ｘビット分を着目中のビットデータと同一にして他のビットを「０」としたＮビットのビット列をＩＤとして、そのマスク用ビットとＩＤとを一組としてメモリ等の記憶媒体の一領域に保存し（ステップＳ４０９）、ステップＳ４１０の判断を行う。

【０１１０】また、ステップＳ４０６の結果、カウント数が２の（Ｎ－Ｘ）乗でない場合には（ステップＳ４０７）、ＴＲＬ生成部１１２は、ステップＳ４０６におけるその条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「０」のものが２個以上存在すれば、着目中のビットデータの下位に１ビットの「０」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ４１１）、その条件を満たす端末ＩＤのうち上位からＸ＋１ビット目が「１」のものが２個以上存在すれば、着目中のビットデータの下位に１ビットの「１」を加えて形成されるビットデータを作業用ビット領域に格納し（ステップＳ４１２）、ステップＳ４１０の判断を行う。

【０１１１】ステップＳ４１０では、ＴＲＬ生成部１１２は、未着目のＸビットのビットデータが存在するか否かを判定し、未着目のＸビットのビットデータが未だ存在すればステップＳ４０５に戻って次のビットデータに着目して処理を行い、未着目のＸビットのビットデータが存在しなければ変数Ｘを１増加し（ステップＳ４１３）、変数ＸがＮと等しいか否かを判定する（ステップＳ４１４）。

【０１１２】ＴＲＬ生成部１１２は、ステップＳ４１４において変数ＸがＮと等しくないと判定した場合には、再びステップＳ４０５に戻って次のビットデータに着目

して処理を行い、変数ＸがＮと等しいと判定した場合には、ＴＲＬ用データ生成処理を終了する。なお、実施の形態３においては、図５のステップＳ２３で示すＴＲＬの構築は、上述のＴＲＬ用データ生成処理によって記憶媒体の一領域に保存されたＩＤとマスク用ビットとの１個又は複数個の組にエントリ数を付加したものと、例外ＩＤにエントリ数を付加したものと、更にバージョン、発行者情報、無効化端末数及び署名情報を加えることによって実行される。

【０１１３】＜ＴＲＬ照合処理＞図１９は、実施の形態３におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。コンテンツ鍵配信装置１２０の照合部１２６は、端末から送られた端末ＩＤを送信要求受付部１２５より得る度にこのＴＲＬ照合処理を行う。

【０１１４】照合部１２６は、端末から送られた端末ＩＤと、ＴＲＬの端末ＩＤ関連情報中のＩＤとマスク用ビットとの組のいずれかで表される端末ＩＤとが一致するかを検査する（ステップＳ４２１～Ｓ４２４）。即ち、照合部１２６は、ＴＲＬ中の１つの未着目のマスク用ビットに着目し、そのマスク用ビットの値に応じたマスクデータを上述したように導出して（ステップＳ４２１）、端末から送られた端末ＩＤと、導出したマスクデータとのビット毎の論理積を求めて（ステップＳ４２２）、求めた論理積が着目中のマスク用ビット４４３と組をなすＩＤ４４２と一致するか否かを判定する（ステップＳ４２３）。

【０１１５】ステップＳ４２３の判定の結果、一致する場合には、照合部１２６は、端末から送られた端末ＩＤがＴＲＬ中の例外ＩＤのいずれかと一致するかを検査し（ステップＳ４２６）、例外ＩＤのいずれとも一致しなければ、端末から取得した端末ＩＤは無効化端末の端末ＩＤであると判定し（ステップＳ４２７）、ＴＲＬ照合処理を終了する。ステップＳ４２６の検査の結果、例外ＩＤのいずれかと一致すると判明した場合には、照合部１２６は、端末から取得した端末ＩＤは無効化端末の端末ＩＤでないと判定し（ステップＳ４２５）、ＴＲＬ照合処理を終了する。

【０１１６】また、ステップＳ４２３において、求めた論理積が着目中のマスク用ビット４４３と組をなすＩＤ４４２と一致しない場合には、照合部１２６はＴＲＬ中の全てのマスク用ビット４４３に着目してステップＳ４２１～Ｓ４２３の処理を行なったかを判定し（ステップＳ４２４）、全てのマスク用ビット４４３に着目して処理を行っていない場合にはステップＳ４２１に戻って未着目のマスク用ビットに着目して処理を行う。

【０１１７】ステップＳ４２４において、全てのマスク用ビットについて処理済みであると判定した場合には、照合部１２６は、端末から取得した端末ＩＤは無効化端末の端末ＩＤでないと判定し（ステップＳ４２５）、ＴＲＬ照合処理を終了する。

＜考察＞実施の形態３に示したコンテンツ鍵配信システムによれば、例えば、その端末ＩＤの上位のいくらかの桁数のビット列が同値であるところの連続したシリアル番号の数十台の端末のうち、数台を除いく他の全てが無効化端末であるような場合において、その同値であるビット列を含むＩＤをＴＲＬの端末ＩＤ関連情報中のＩＤとし、その同値である部分の桁数を示す値をそのＩＤと組をなすマスク用ビットとして定め、その数台についての端末ＩＤを端末ＩＤ関連情報中の例外ＩＤとして定めたＴＲＬによって無効化端末を特定することが可能となるため、ＴＲＬのデータ量を少なく抑えることができるようになる。

＜実施の形態４＞以下、実施の形態４に係るコンテンツ鍵配信システムについて説明する。

【０１１８】図２０は、本発明の実施の形態４に係るコンテンツ鍵配信システムの構成図である。実施の形態１で示したコンテンツ鍵配信システム１００における管理装置１１０は、ＴＲＬを通信路を通じてコンテンツ鍵配信装置１２０に対して送信するものであったのに対し、この実施の形態４に係るコンテンツ鍵配信システム５００においては管理装置５１０はＴＲＬを光磁気ディスク等の記録媒体５０１に記録し、コンテンツ鍵配信装置５２０がその記録媒体５０１からＴＲＬを読み出すようになっている。

【０１１９】図２０においては、実施の形態１で示した構成要素（図１参照）と基本的に同等のものについては同一の符号を用いて表しており、その構成要素についてはここでは詳しく説明しない。管理装置５１０は、例えばコンテンツの著作権等の保護に関する業務を行う機関に設置されるコンピュータ等であり、各端末１３０のうち、内部に記憶されている復号鍵が暴露される等により著作権等の保護が図れない事態に陥っている全ての端末、即ち暗号化コンテンツ鍵の配信先にすべきでない全ての端末を、特定するための情報を主たる内容とするＴＲＬを生成して記録媒体に記録する処理を行う装置であり、無効化端末ＩＤ群取得部１１１、ＴＲＬ生成部１１２及びＴＲＬ記録部５１３を備え、光磁気ディスク等の記録媒体５０１を装着できる。

【０１２０】ここで、ＴＲＬ生成部１１２は、無効化端末ＩＤ群取得部１１１から与えられた各端末ＩＤに基づいて無効化端末を特定する情報を主たる内容とするＴＲＬを生成し、ＴＲＬ記録部５１３に伝える機能を有する。また、ＴＲＬ記録部５１３は、ＴＲＬ生成部１１２から伝えられたＴＲＬを管理装置５１０に装着された記録媒体５０１に記録する機能を有する。

【０１２１】この管理装置５１０は、図５に示すステップＳ２４をＴＲＬを記録媒体に記録する処理に置き換えた内容のＴＲＬ生成送信処理を行う。管理装置５１０に

よってＴＲＬが記録された記録媒体５０１は、人手を介してコンテンツ鍵配信装置５２０に配送される。例えば、新たな内容のＴＲＬが生成される毎に、ＴＲＬは記録媒体に記録され、コンテンツ鍵配信装置まで配送される。

【０１２２】コンテンツ鍵配信装置５２０は、各端末からの暗号化コンテンツ鍵の送信要求を受けるとその端末が無効化端末でない場合に限りその端末に暗号化コンテンツ鍵を送信することを内容とするコンテンツ鍵配信処理を行うコンピュータであり、機能的には、ＴＲＬ格納部１２１、ＴＲＬ読出部５２２、コンテンツ鍵記憶部１２３、暗号化鍵群記憶部１２４、送信要求受付部１２５、照合部１２６、暗号化部１２７及び暗号化コンテンツ鍵送信部１２８を備え、光磁気ディスク等の記録媒体５０１を装着できる。

【０１２３】ここで、ＴＲＬ読出部５２２は、コンテンツ鍵配信装置５２０に装着された記録媒体５０１からＴＲＬを読み出してＴＲＬ格納部１２１に格納する機能を有する。従って、このコンテンツ鍵配信システム５００においては、管理装置５１０とコンテンツ鍵配信装置５２０とが通信路で接続されていなくても、記録媒体を介してＴＲＬの伝達が実現される。

【０１２４】なお、この実施の形態４において用いられるＴＲＬは実施の形態１～３のいずれで示したものであってもよく、コンテンツ鍵配信装置がそのＴＲＬの構造に応じたＴＲＬ照合処理等を行うこととすればよい。

＜補足＞以上、本発明に係る暗号通信システムについて、コンテンツ鍵配信システムとして適用した実施の形態１～４を示して説明したが、本発明はこのような実施の形態に限られないことは勿論である。即ち、

（１）実施の形態１～３では、管理装置とコンテンツ鍵配信装置との間でＴＲＬを配信するための通信路を示し、実施の形態４では、ＴＲＬの配送に用いる記録媒体を示したが、管理装置とコンテンツ鍵配信装置との間は、通信路と記録媒体とを合わせて用いることによってＴＲＬが伝送されるようになっていてもよい。例えば、管理装置から別のある通信装置までは記録媒体でＴＲＬが配送され、その通信装置からコンテンツ鍵配信装置までは通信路を通じてＴＲＬが配信されることとしてもよい。

（２）各実施の形態で示したコンテンツ再生装置は、必ずしも暗号化コンテンツを予め入手してからコンテンツ鍵配信装置に送信要求を送られければならないのではなく、例えば、コンテンツ鍵を取得した後に、暗号化コンテンツを入手してその再生を行うこととしてもよい。

（３）各実施の形態で示したコンテンツ再生装置は、その装置固有の端末ＩＤと、その装置固有の復号鍵を保持していることとし、コンテンツ鍵配信装置は全ての復号鍵に呼応する暗号化鍵を保持していることとしたがたが、コンテンツ再生装置が複数の復号鍵を備え、各復号鍵を識別するための復号鍵ＩＤを送信要求に含めてコンテンツ鍵配信装置に送り、また、コンテンツ鍵配信装置は全ての復号鍵に呼応する暗号化鍵を復号鍵ＩＤと対応付けて保持しておき、その送られた復号鍵ＩＤに対応する暗号化鍵を用いてコンテンツ鍵をコンテンツ再生装置に送信することとしてもよい。なお、この場合には、各実施の形態で示したＴＲＬの端末ＩＤ関連情報によって、無効化端末の端末ＩＤの代わりに、無効化すべき復号鍵に対応する復号鍵ＩＤを特定するようにし、ＴＲＬ照合処理等において端末ＩＤの代わりに復号鍵ＩＤを照合対象とすることすればよい。

【０１２５】なお、コンテンツ再生装置に着脱可能なＩＣカード等に、復号鍵及び復号鍵ＩＤが記録されていることとしてもよい。

（４）実施の形態１～３では管理装置のＴＲＬ生成部１１２が、ＴＲＬ用データ生成処理（図１０、図１４、図１８）等によりＴＲＬを自動生成することとしたが、ＴＲＬの端末ＩＤ関連情報を生成するアルゴリズムはこれに限定されることはない。また、ＴＲＬは、オペレータ等の入力操作を受けて生成されることとしてもよいし、また外部装置において生成されたＴＲＬを管理装置内に取得してからＴＲＬ送信部１１３でそのＴＲＬを配信することとしてもよい。

【０１２６】また、コンテンツ鍵配信システムにおいて管理装置が複数存在することとしてもよく、ある管理装置から他の管理装置にＴＲＬを伝送しておくこととしてもよい。また、コンテンツ鍵配信装置の方から管理装置に要求を出したときに、管理装置がＴＲＬの送信を行うこととしてもよく、コンテンツ鍵配信装置は定期的又は端末から送信要求があったときにＴＲＬの送信を管理装置に要求することとしてもよい。

（５）実施の形態２で示した端末ＩＤのデータ構成は、必ずしも図１２に示した内容である必要はない。但し、メーカーや、製品等を表すビット列を端末ＩＤ中に含ませておくことにより、あるメーカーの製造した端末全てが無効化端末となる場合等にＴＲＬのデータ量を小さくすることができるようになる。

【０１２７】なお、実施の形態２では、上位のビット列でメーカーＩＤを表すものとして端末ＩＤを定義した例を示したが、端末ＩＤ中の下位のビット列を、メーカーＩＤを表すものとして端末ＩＤを定義してもよいし、端末ＩＤ中の上位と下位との間のビット列を、メーカーＩＤを表すものとして端末ＩＤを定義してもよい。

（６）実施の形態２で示したＴＲＬの端末ＩＤ関連情報中のマスク用ビットは、例えば８ビット等と固定長データとしたが、可変長データとして、そのデータ長を示す情報と対にしておくこととしてもよい。

（７）実施の形態３で示したＴＲＬ用データ生成処理の結果として得られた端末ＩＤ関連情報に関して、端末ＩＤが１２８ビットとした場合において、例外ＩＤから最

下位ビットを０としたＩＤとマスク用ビットが１２７という値を示す一組が端末ＩＤ関連情報中に存在するときには、その一組及びその例外ＩＤを削除して、その例外ＩＤの最下位ビットを反転したものをＩＤとしてマスク用ビットを１２８とした一組を端末ＩＤ関連情報中に追加することとしてもよい。

【０１２８】また、実施の形態３では、各例外ＩＤは、１つの端末ＩＤを示すものとしたが、図１７に示した例外ＩＤの代わりに、例外ＩＤと例外マスク用ビットとの組を１個又は複数個含む例外グループ情報をＴＲＬの端末ＩＤ関連情報中に含めることとしてもよい。即ち、ＩＤ４４２とマスク用ビットとの組の全てで示される端末ＩＤ群の中から、その例外ＩＤと例外マスク用ビットとの組の全てで示される端末ＩＤ群を除いたものが、全ての無効化端末の端末ＩＤであるように端末ＩＤ関連情報を構成することとしてもよい。

（８）実施の形態１～４では、本発明に係る暗号通信システムが、コンテンツ鍵配信システムに適用された場合の例を示したが、端末からの端末ＩＤを受けてその端末が無効化端末か否かを判定してその判定結果に応じて何らかの通信処理の実行可否を決定するような通信システムであれば、特にその通信処理内容は、暗号化コンテンツ鍵の送信に限るものではない。例えば、無効化端末か否かの判定の結果に応じて、端末側から端末固有の暗号化を施して送られる重要データを受け付ける処理の実行可否を決定することとしてもよい。

（９）実施の形態１～３で示したコンテンツ鍵配信システムの処理手順（図５～７、図１０、図１１、図１４、図１６、図１８、図１９に示した手順等）を、コンピュータ等に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ＩＣカード、光ディスク、フレキシブルディスク、ＲＯＭ等がある。流通、頒布されたコンピュータプログラムは、コンピュータ等にインストール等されることにより利用に供され、そのコンピュータ等は当該コンピュータプログラムを実行して、実施の形態１～３で示したような各種処理を行うことができるようになる。

【０１２９】

【発明の効果】以上の説明から明らかように、本発明に係る暗号通信システムは、暗号通信装置と、自端末装置を識別可能な所定ビット数のビット列なる端末識別子を、当該暗号通信装置に送信する機能を有する複数の端末装置と、無効化すべき端末装置を特定するものとして１以上の端末識別子を示す無効化端末特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化端末特定情報を取得する無効化端末特定情報取得手段と、端末装置から端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、一方、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを有することを特徴とする。

【０１３０】ここで、暗号通信装置は、例えば実施の形態１～３で示すようなコンテンツ鍵配信装置であり、所定の通信とは例えば暗号化コンテンツ鍵の送信であり、無効化端末特定情報は例えば実施の形態１～３において示すＴＲＬである。本発明により、あるビット列を含む全ての端末ＩＤを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、ＴＲＬのデータ量を比較的小さく抑えることができるようになり、この結果、一部の無効化すべき端末装置を除いた適切な端末装置に対してのみ、コンテンツ鍵を暗号化して配信する等の暗号通信に係るサービスを行う実用的な暗号通信システムが実現される。

【０１３１】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定する

こととしてもよい。

【０１３２】これにより、無効化端末特定情報を、端末ＩＤの一部の値とその一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末ＩＤを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【０１３３】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列である代表値情報と、所定ビット数のマスクフラグとを対応付けて１組以上含んでおり、端末識別子中の部分のうち各マスクフラグにおけるビット値が１である部分の値が、当該マスクフラグに対応する代表値情報における当該部分の値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各マスクフラグについて、前記端末識別子受信手段により受信された端末識別子と当該マスクフラグとの論理積と、当該マスクフラグに対応する代表値情報と当該マスクフラグとの論理積とが一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【０１３４】これにより、端末ＩＤの一部の値とその一部のビット位置との組で、多数の端末ＩＤを表す方式において、その一部を構成するビット位置を、マスクフラグ中の値を１とした位置で示して、その一部を構成しないビット位置を、マスクフラグ中の値を０とした位置で示すことになる。従って、端末から受信した端末ＩＤのうち、無効化端末特定情報中に含まれる値と照合すべき部分を、その端末ＩＤとマスクフラグとの論理積を求めるという計算量の小さい簡易な演算によって抽出することができるようになる。このことは、暗号通信装置における判定の高速化につながる。

【０１３５】また、前記無効化端末特定情報生成手段は、前記無効化端末特定情報に所定ビット数の孤立値情報を含めて生成し、前記無効化端末特定情報は、更に前記孤立値情報と同一の値を有する端末識別子をも、無効化すべき端末装置として特定する情報であり、前記判定手段は更に、前記端末識別子受信手段により受信された端末識別子と、前記無効化端末特定情報に含まれる孤立値情報とが一致する場合にも、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【０１３６】ここで孤立値情報は、例えば図８で示す個別情報であり、これにより、一の無効化端末の端末ＩＤが、他の無効化端末の端末ＩＤと共通するビットを持たない場合、つまり孤立している場合において、その一の無効化端末の端末ＩＤを孤立値情報として無効化端末特定情報に含ませているため、孤立した無効化端末が多い場合には、その一の無効化端末の端末ＩＤを、その端末ＩＤの値と全ビットが１であるマスクフラグとの組で表現した形式よりも、少量のデータで無効化端末特定情報を構成することができる。

【０１３７】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、ビット桁数を示す有効上位桁情報と、当該ビット桁数分のビット列の値を示す値情報とを対応付けて１組以上含んでおり、端末識別子中の最上位ビットから各有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各有効上位桁情報について、前記端末識別子受信手段により受信された端末識別子中の最上位ビットから当該有効上位桁情報により示されるビット桁数分のビット列の値が、当該有効上位桁情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【０１３８】これにより、端末ＩＤの上位から任意のビット数分だけ共通な値を持つ全ての端末ＩＤを、そのビット数を示す有効上位桁情報と値情報とにより表すことができる。一般に端末ＩＤの管理運用上、端末を製造したメーカー識別子等、ある程度端末の構造や機能に共通な性質を有するまとまりを区別する情報が端末ＩＤの上位ビットに位置付けることが多いことから、これにより、特定のメーカーや製品構造等に関連して無効化すべき端末が多数発生した場合において、比較的少量のデータで無効化端末特定情報を構成することができるようになる。

【０１３９】また、前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、前記無効化端末特定情報生成手段は、前記所定ビット数をＮとすると、前記端末識別子取得手段により取得された端末識別子のうち最上位ビットからＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値を１以上特定し、各Ｘの値について、当該条件に係る２の（Ｎ－Ｘ）乗個の端末識別子を、Ｘなるビット桁数を示す有効上位桁情報と、当該端末識別子の最上位ビットからＸビットの部分のビット列の値を示す値情報とでもって包括的に表現し

41

たデータ形式を用いて前記無効化端末特定情報を生成することとしてもよい。

【０１４０】これにより、管理装置のオペレータ等に特段の操作負担をかけることなく、データ量を抑えた無効化端末特定情報を構築することができるようになる。また、前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の最上位ビットから所定ビット数のビット列で当該端末装置の製造者を示すこととしてもよい。

【０１４１】これにより、上位から一定のビット数分が共通である全ての端末ＩＤを一組の小さな情報で表すことが可能であり、端末ＩＤの上位にメーカーを示す情報が含まれるため、特定のメーカーが製造した端末に機構上の問題、例えばユーザが一定手順を実行することにより無制限にコンテンツをコピーできるような欠陥があることが判明した場合等において、無効化端末特定情報のデータ量を効果的に抑えることができるようになる。

【０１４２】また、前記各端末装置を識別する各端末識別子は、当該端末識別子中の前記製造者を示すビット列に続く上位の所定数のビット列で、当該端末装置が如何なる種別の製品に属するかを示すこととしてもよい。これにより、特定メーカーの製造した一定の製品のみに問題があることが判明した場合において、その製品が実装された全ての端末を無効化端末とするために必要な無効化端末特定情報のデータ量を抑えることが可能となる。

【０１４３】また、前記複数の端末装置は各々固有の復号鍵を保持しており、更にコンテンツ鍵で暗号化されたコンテンツである暗号化コンテンツを自端末装置内部に格納可能であり、前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段と、前記コンテンツ鍵を記憶するコンテンツ鍵記憶手段とを有し、前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行い、前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて前記コンテンツ鍵を暗号化して送信し、前記端末装置は、暗号通信装置から送信された暗号化済みのコンテンツ鍵を自端末装置固有の前記復号鍵を用いて復号する復号手段と、前記暗号化コンテンツが自端末装置内部に格納されている場合において前記復号手段により復号されたコンテンツ鍵を用いて当該暗号化コンテンツを復号して再生する再生手段とを有することとしてもよい。

【０１４４】これにより、端末は暗号化コンテンツ鍵を

42

暗号通信装置から取得した場合に限ってコンテンツの再生が可能になることとして著作権保護等に配慮したシステムを実現する場合において、あるメーカーの製造した一群の端末が著作権保護不可能な状態に陥ったことが判明したときに、端末ＩＤ中の上位からメーカーＩＤの部分までを示すビット桁数及びそのメーカーＩＤという少ないデータ量のデータでその一群の無効化すべき端末を識別するための情報を構成することができるため、管理装置から暗号通信装置に送信しなければならないデータのデータ量を抑えることができ、そのデータの送信時間が短縮できる。

【０１４５】また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値及び当該部分を特定する包括情報を１以上含み、かつ、所定ビット数の例外情報を１以上含んでおり、端末識別子中の部分のうち各包括情報により特定される部分が当該包括情報により特定される値と同一である全ての端末識別子のうちから、前記各例外情報と同値である端末識別子を除いたものの全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記端末識別子受信手段により受信された端末識別子が、前記無効化端末特定情報に含まれるいずれかの包括情報により特定される部分において当該包括情報により特定される値と一致するか否かを検査し、当該検査において一致した場合には、当該受信された端末識別子が前記無効化端末特定情報に含まれるいずれかの例外情報と同値である場合を除いて、当該端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【０１４６】これにより、単に包括情報のみで無効化端末の端末ＩＤを特定するより、例外情報を用いていることによって、少ないデータ量で全ての無効化端末の端末ＩＤを特定することができる場合がある。例えば、無効化端末が１５台あり、その端末ＩＤはいずれも下位４ビットを除く全てのビット列の値が共通している状況を想定すれば、仮に、１つの包括情報によって、下位３ビットを除く全てのビット列の値が共通する８個の端末ＩＤを表現し、別の１つの包括情報によって、下位２ビットを除く全てのビット列の値が共通する４個の端末ＩＤを表現し、更に別の１つの端末ＩＤの値自体によってその端末ＩＤを表現することとして合計１５台の無効化端末の端末ＩＤを特定する無効化端末特定情報を構築する場合に比べて、本発明によれば、例えば１つの包括情報によって、下位４ビットを除くビット列が共通する１６個の端末ＩＤを表現し、例外情報によって、その１６個の端末ＩＤのうち無効化端末でない１台の端末の端末ＩＤを表現することとして同じ意味の無効化端末特定情報を構築することができるので、無効化端末特定情報のデータ量を抑えることができる。

【０１４７】また、前記管理装置は、無効化すべき全ての端末装置の端末識別子を取得する端末識別子取得手段を有し、前記無効化端末特定情報生成手段は、前記所定ビット数をＮとすると、前記端末識別子取得手段により取得されたいずれかの端末識別子の最下位ビットのみ反転したＮビットのビット列であって、当該端末識別子取得手段により取得された他のいずれかの端末識別子とも値が同一でないという条件を満たすビット列を、前記例外情報と定めるとともに、当該ビット列を端末識別子とみなし、前記端末識別子取得手段により取得された端末識別子及び前記みなした端末識別子のうち、最上位ビットからＸビットの値が同一である端末識別子の個数が２の（Ｎ－Ｘ）乗であるという条件を満たすＸの値で、かつ、Ｎ未満であるＸの値を、１以上特定し、特定した各Ｘの値について、当該Ｘの値と、当該条件に係る２の（Ｎ－Ｘ）乗個の端末識別子の最上位ビットからＸビットの部分のビット列の値とを特定する情報を前記包括情報と定めることにより前記無効化端末特定情報を生成することとしてもよい。

【０１４８】これにより、管理装置のオペレータ等に特段の操作負担をかけることなく、一定の状況においてデータ量を抑えた無効化端末特定情報を構築することができるようになる。また、前記複数の端末装置は各々固有の復号鍵を保持しており、前記暗号通信装置は、全ての前記端末装置の復号鍵に呼応する暗号化鍵を記憶する暗号化鍵記憶手段を有し、前記通信手段は、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置に対して、当該端末装置の復号鍵に呼応する暗号化鍵を用いて通信データを暗号化して送信し、前記端末装置は、暗号通信装置から送信された通信データを自端末装置固有の前記復号鍵を用いて復号することとしてもよい。

【０１４９】これにより、正常な端末に対してのみに、通信データを送信するサービスを行う暗号通信装置を含むシステムにおいて、無効化すべき端末が多数発生したような事態においても、端末が正常なものであるか否かの判断に必要な無効化端末特定情報のデータ量を小さく抑えることができるため、その判断の迅速化等が図れるようになる。

【０１５０】また、前記出力手段は、前記無効化端末特定情報を暗号通信装置に対し送信することにより前記出力を行い、前記無効化端末特定情報取得手段は、前記出力手段により送信された前記無効化端末特定情報を受信することにより前記取得を行うこととしてもよい。これにより、管理装置は、暗号通信装置が必要とする無効化端末特定情報をデータ量を抑えて構築して、迅速に暗号通信装置に伝送することが可能になる。

【０１５１】また、前記出力手段は、記録媒体を装着可能な装着部を有し、装着された記録媒体に前記無効化端末特定情報を記録することにより前記出力を行い、前記無効化端末特定情報取得手段は、前記記録媒体を装着可能であり、装着された記録媒体から前記無効化端末特定情報を読み出すことにより前記取得を行うこととしてもよい。

【０１５２】これにより、管理装置が、暗号通信装置が必要とする無効化端末特定情報を記録媒体に記録して伝達する場合において、ある程度小さい記録許容容量の従来の記録媒体を利用することができるようになる。また、本発明に係る管理装置は、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき１以上の各端末装置の各端末識別子を示す無効化端末特定情報を生成する管理装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記無効化端末特定情報を生成する無効化端末特定情報生成手段と、生成された前記無効化端末特定情報を出力する出力手段とを備えることを特徴とする。

【０１５３】この管理装置によって、出力される無効化端末特定情報は比較的小さいデータ量で多数の無効化端末を特定することができるものとなり、その出力される無効化端末特定情報は、伝送や記録媒体への記録の面において、利用しやすいものとなる。また、前記無効化端末特定情報生成手段により生成される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であることとしてもよい。

【０１５４】これにより、無効化端末特定情報を、端末ＩＤの一部の値とその一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末ＩＤを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【０１５５】また、前記各端末装置は、複数の製造者のうちいずれかにより製造されたものであり、前記各端末装置を識別する各端末識別子は、当該端末識別子中の所定範囲のビット列で当該端末装置の製造者を示すこととしてもよい。これにより、特定のメーカーが製造した端末に機構上の欠陥あることが判明した場合等において、無効化端末特定情報のデータ量を効果的に抑えることが

できるようになる。

【０１５６】また、本発明に係る暗号通信装置は、複数の端末装置のうち自端末装置を識別可能な所定ビット数のビット列なる端末識別子を保持する各端末装置との間で通信を行う暗号通信装置であって、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて構成され、無効化すべき端末装置を特定するためのものとして１以上の各端末装置の各端末識別子を示した無効化端末特定情報を外部から取得する無効化端末特定情報取得手段と、端末装置から、当該端末装置が保持する端末識別子が送信された場合に当該端末識別子を受信する端末識別子受信手段と、前記端末識別子受信手段により受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致するか否かを判定する判定手段と、前記受信された端末識別子が前記無効化端末特定情報により示される何れの端末識別子とも一致しないと前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間で、当該端末装置に固有な暗号化を施すことにより所定の通信を行い、前記受信された端末識別子が前記無効化端末特定情報により示される何れかの端末識別子と一致すると前記判定手段により判定された場合には、当該端末識別子を送信した端末装置との間では前記所定の通信を行わない通信手段とを備えることを特徴とする。

【０１５７】これにより、比較的小さいデータ量で多数の無効化端末を特定する無効化端末特定情報を取得して参照し、端末から受信した端末ＩＤが無効化端末の端末ＩＤであるか否かの判定を迅速に行うことができるようになる。また、前記無効化端末特定情報取得手段により取得される前記無効化端末特定情報は、所定ビット数のビット列中の一部分の値を示す値情報と、当該ビット列中における当該部分のビット位置を特定するための位置情報とを対応付けて１組以上含んでおり、端末識別子中の部分的なビット列であって各位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と同一である全ての端末識別子それぞれによって識別される端末装置の全てを、無効化すべき端末装置として特定する情報であり、前記判定手段は、前記無効化端末特定情報に含まれる各位置情報について、前記端末識別子受信手段により受信された端末識別子中の当該位置情報により特定されるビット位置に所在する部分的なビット列の値が、当該位置情報に対応する値情報で示される値と一致するか否かを検査し、当該検査において一度でも一致した場合には、当該受信された端末識別子が、無効化すべき端末装置を特定するものとして前記無効化端末特定情報により示される何れかの端末識別子と一致すると判定することとしてもよい。

【０１５８】これにより、無効化端末特定情報を、端末ＩＤの一部の値とその一部の位置とを対応付けている形式としたため、一部の位置を運用ルール等で固定的に決めておく必要なく、任意のビット列範囲についてその範囲の値が共通な全ての端末ＩＤを一組の値及び位置からなる情報で表し得るため、効果的に運用すれば、多数の無効化端末を少ない情報量で表すことができるようになる。

【０１５９】また、本発明に係る情報生成方法は、複数の端末装置のうち無効化すべき端末装置を特定するための無効化端末特定情報を生成する情報生成方法であって、前記複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を取得する端末識別子取得ステップと、前記所定ビット数のビット列中の一部分の値を特定する情報により当該部分が当該値と同一である全ての端末識別子を包括的に表現するデータ形式を用いて、前記端末識別子取得ステップにより取得された全ての端末識別子を示す前記無効化端末特定情報を生成する生成ステップとを含むことを特徴とする。

【０１６０】これにより、多数の無効化端末を特定するための情報を小さいデータ量に抑えて構築することができるようになる。また、本発明に係る記録媒体は、無効化端末特定データを記録したコンピュータ読み取り可能な記録媒体であって、前記無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする。同様に、本発明に係る無効化端末特定データは、複数の端末装置それぞれを識別可能な所定ビット数のビット列なる端末識別子のうち、無効化すべき各端末装置の各端末識別子を特定するために、前記所定ビット数のビット列中の一部分の値を特定するための部分特定情報を記録した端末識別子特定フィールドを有し、当該部分特定情報により、当該部分が当該値と同一である全ての端末識別子を包括的に表現していることを特徴とする。

【０１６１】これらにより、あるビット列を含む全ての端末ＩＤを、それに含まれる共通するビット列の値と位置とを特定する情報で包括的に表現するので、無効化端末特定データのデータ量を比較的小さく抑えることができるようになる。また、本発明に係る暗号通信システムは、暗号通信装置と、当該暗号通信装置に所定ビット数の鍵識別子を送信する端末装置と、無効化すべき１以上の各鍵識別子を特定する無効化鍵識別子特定情報を生成する管理装置とを備える暗号通信システムであって、前記管理装置は、前記所定ビット数のビット列中の一部分

の値を特定する情報により当該部分が当該値と同一である全ての鍵識別子を包括的に表現するデータ形式を用いて、前記無効化鍵識別子特定情報を生成する無効化鍵識別子特定情報生成手段と、生成された前記無効化鍵識別子特定情報を出力する出力手段とを有し、前記暗号通信装置は、前記管理装置により出力された前記無効化鍵識別子特定情報を取得する無効化鍵識別子特定情報取得手段と、端末装置から鍵識別子を受信する鍵識別子受信手段と、前記鍵識別子受信手段により受信された鍵識別子が、前記無効化鍵識別子特定情報により特定される何れかの鍵識別子と一致するか否かを判定する判定手段と、前記受信された鍵識別子が前記無効化鍵識別子特定情報により特定される何れの鍵識別子とも一致しないと前記判定手段により判定された場合に限って、当該鍵識別子を送信した端末装置との間で、当該鍵識別子について固有な暗号化を施すことにより所定の通信を行う通信手段とを有することを特徴とする。

【０１６２】これにより、正当な鍵識別子を送った端末に対してのみ、特定の重要なデータの送信等といった所定の通信を行うようなサービスを行うシステムにおける、鍵識別子の正当性の確認に要するデータのデータ量を抑えることができるので、かかるシステムの実用性を高めることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るコンテンツ鍵配信システムの構成図である。

【図２】各端末が記憶している端末ＩＤと復号鍵とを示す図である。

【図３】各端末が保持する端末ＩＤの値の決定方法を示す概念図である。

【図４】コンテンツ鍵配信装置１２０の暗号化鍵群記憶部１２４に記憶されるデータの内容例を示した図である。

【図５】管理装置１１０が行うＴＲＬ生成送信処理を示すフローチャートである。

【図６】コンテンツ再生装置１３０が行うコンテンツ再生処理を示すフローチャートである。

【図７】コンテンツ鍵配信装置１２０が行うコンテンツ鍵配信処理を示すフローチャートである。

【図８】実施の形態１におけるＴＲＬのデータ構成を示す図である。

【図９】ＴＲＬの内容例を示す図である。

【図１０】実施の形態１における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。

【図１１】実施の形態１におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。

【図１２】実施の形態２における端末ＩＤのデータ構成を示す図である。

【図１３】実施の形態２におけるＴＲＬのデータ構成を示す図である。

【図１４】実施の形態２における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。

【図１５】ＴＲＬの内容例を示す図である。

【図１６】実施の形態２におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。

【図１７】実施の形態３におけるＴＲＬのデータ構成を示す図である。

【図１８】実施の形態３における管理装置１１０により行われるＴＲＬ生成送信処理の一部であるＴＲＬ用データ生成処理を示すフローチャートである。

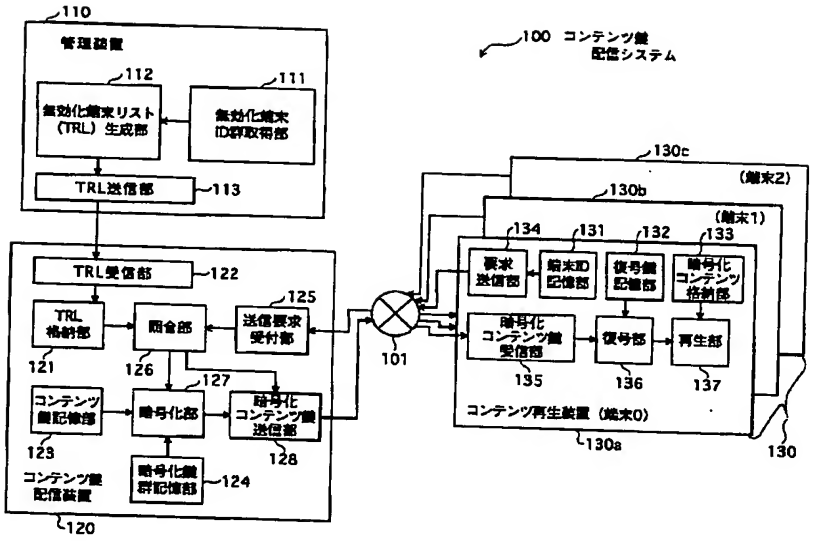
【図１９】実施の形態３におけるコンテンツ鍵配信装置１２０により行われるコンテンツ鍵配信処理の一部であるＴＲＬ照合処理を示すフローチャートである。

【図２０】本発明の実施の形態４に係るコンテンツ鍵配信システムの構成図である。

【符号の説明】

１００　コンテンツ鍵配信システム
１０１　通信路
１１０　管理装置
１１１　無効化端末ＩＤ群取得部
１１２　ＴＲＬ生成部
１１３　ＴＲＬ送信部
１２０　コンテンツ鍵配信装置
１２１　ＴＲＬ格納部
１２２　ＴＲＬ受信部
１２３　コンテンツ鍵記憶部
１２４　暗号化鍵群記憶部
１２５　送信要求受付部
１２６　照合部
１２７　暗号化部
１２８　暗号化コンテンツ鍵送信部
１３０　コンテンツ再生装置（端末）
１３１　端末ＩＤ記憶部
１３２　復号鍵記憶部
１３３　暗号化コンテンツ格納部
１３４　要求送出部
１３５　暗号化コンテンツ鍵受信部
１３６　復号部
１３７　再生部
５００　コンテンツ鍵配信システム
５０１　記録媒体
５１０　管理装置
５１３　ＴＲＬ記録部
５２０　コンテンツ鍵配信装置
５２２　ＴＲＬ読出部

【図１】

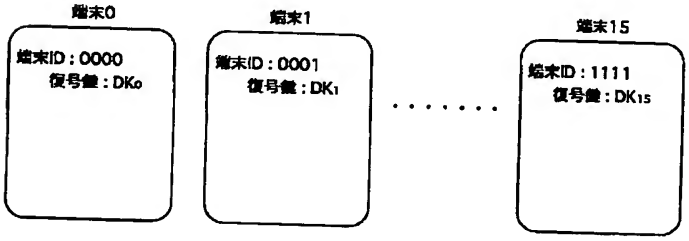


【図４】

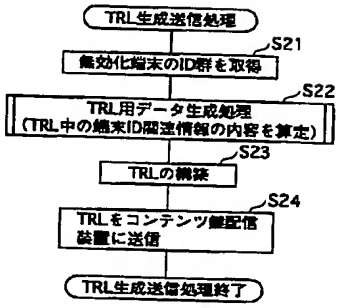
124
暗号化鍵群記憶部

端末ID	暗号化鍵
0000	EK_0
0001	EK_1
0010	EK_2
：	：
1111	EK_{15}

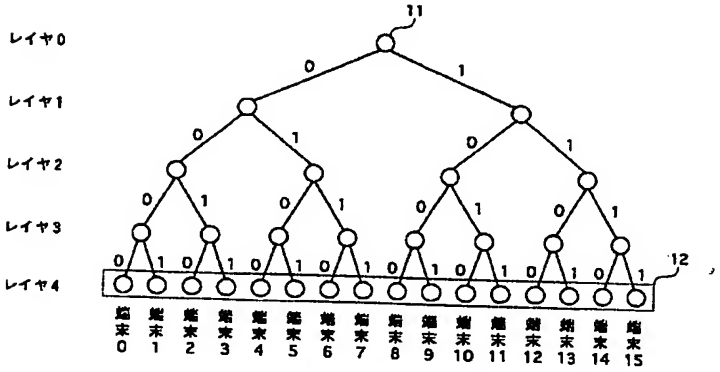
【図２】



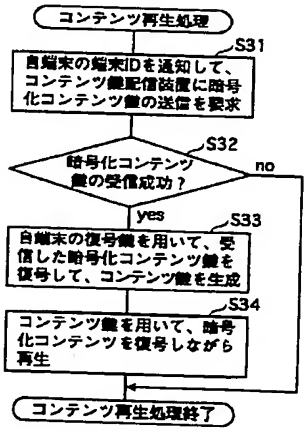
【図５】



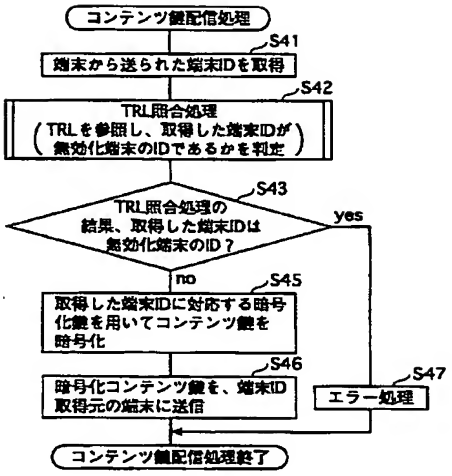
【図３】



【図６】



【図７】



【図８】

TRL

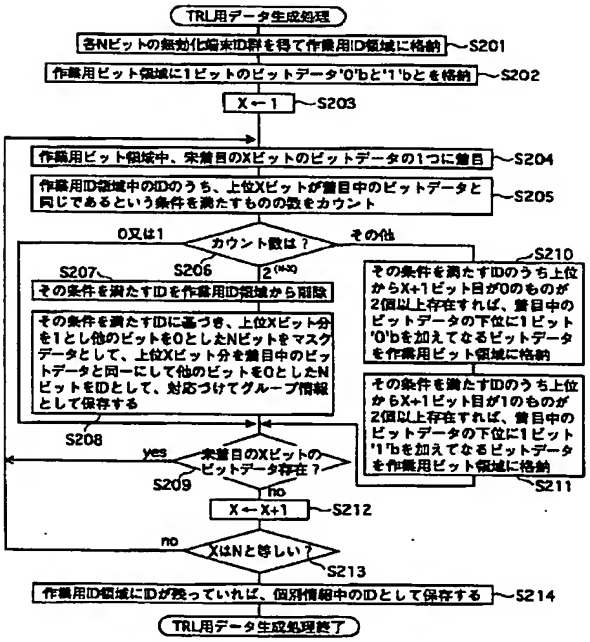
	フィールド		ビットサイズ例 (他の例)	
210	バージョン情報		8 (8)	
220	端末ID関連情報 グループ情報	エントリ数 (M)	4 (128)	222
		M× ID	4 (128)	223
		M× マスクデータ	4 (128)	224
221	端末ID関連情報 個別情報	エントリ数 (N)	4 (128)	226
225		N×ID	4 (128)	227
230	署名情報		64 (320)	

【図９】

TRL内容例

フィールド			内容例
バージョン情報			1
端末ID関連情報	グループ情報	エントリ数	2
		ID	'1100'b
		マスクデータ	'1100'b
		ID	'0110'b
		マスクデータ	'1110'b
	個別情報	エントリ数	1
		ID	'0001'b
署名情報			(上の全フィールドの内容を反映した値)

【図１０】

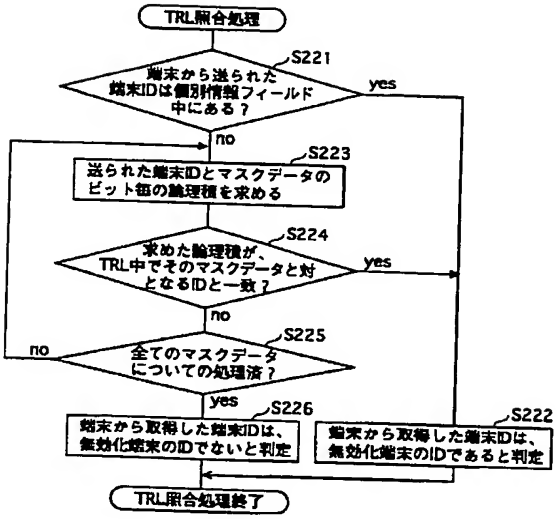


【図１２】

端末ID (128ビット)

	フィールド	ビットサイズ	ビット位置
301	メーカーID	32	0～31
302	製品ID	32	32～63
303	製品バージョンID	32	64～95
304	シリアル番号	32	96～127

【図１１】



【図１３】

TRL

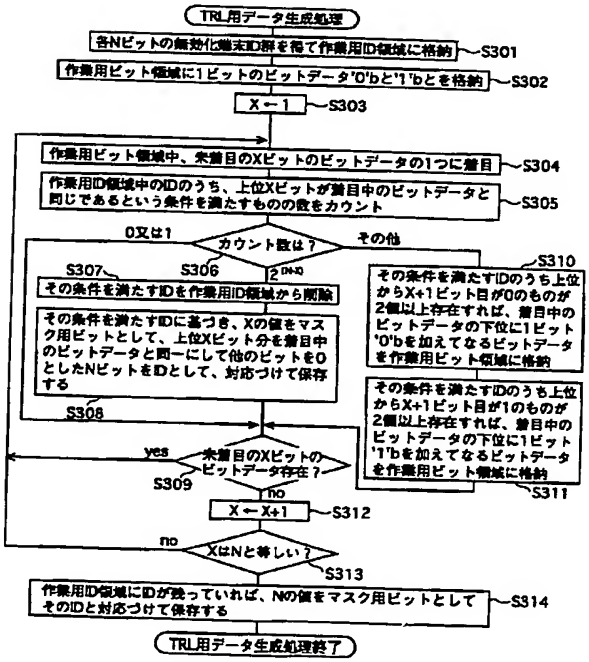
	フィールド		ビットサイズ	
310	バージョン		8	
320	発行者情報		128	
330	無効化端末数		128	
340	端末ID関連情報	エントリ数（N）	32	341
		N×（ID	128	342
		マスク用ビット）	8	343
350	署名情報		320	

【図１５】

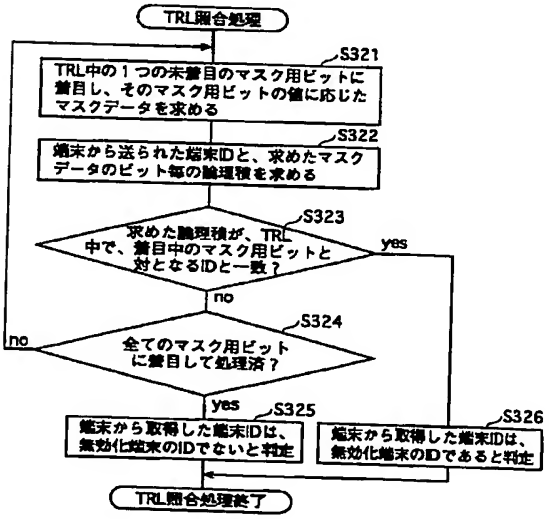
TRL内容例

フィールド		内容例	ビットサイズ
バージョン		1	8
発行者情報		ABC	128
無効化端末数		7	4
端末ID関連情報	エントリ数	3	4
	ID	'1100'b	4
	マスク用ビット	2	2
	ID	'0110'b	4
	マスク用ビット	3	2
	ID	'0001'b	4
	マスク用ビット	4	2
署名情報			320

【図１４】



【図１６】

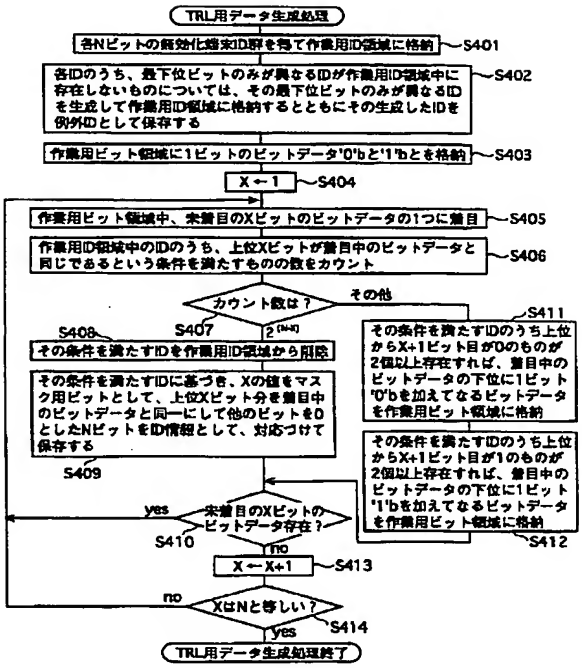


【図１７】

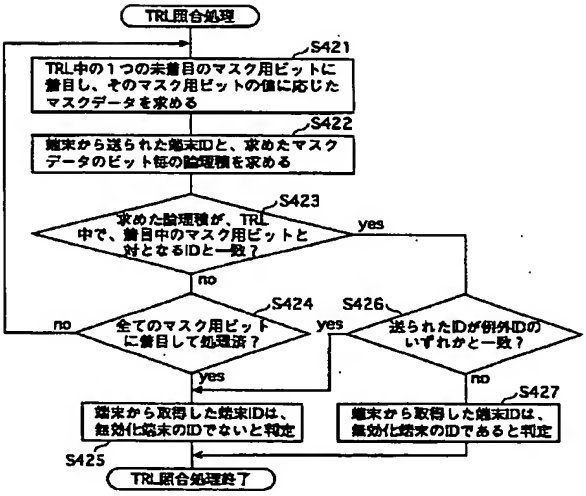
TRL

	フィールド		ビットサイズ	
410	バージョン		8	
420	発行者情報		128	
430	無効化端末数		128	
440	端末ID関連情報	エントリ数（N）	32	441
		N×{ID	128	442
		マスク用ビット}	8	443
		例外エントリ数（M）	32	444
		M×例外ID	128	445
450	署名情報		320	

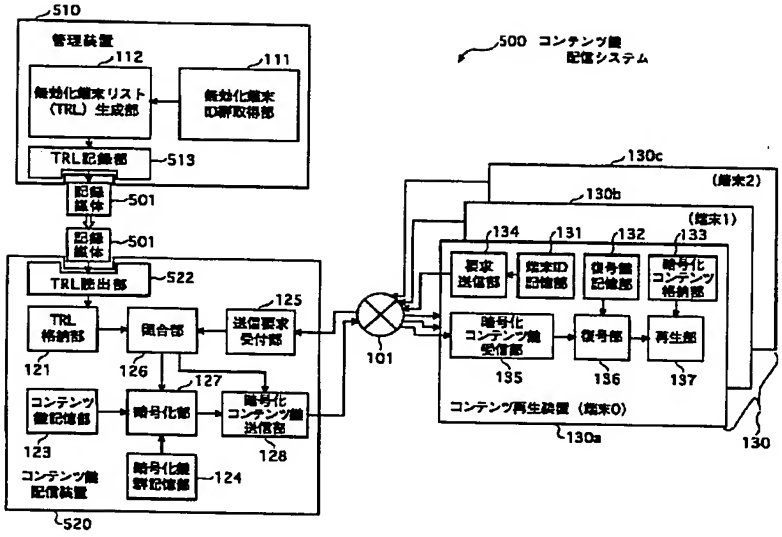
【図１８】



【図１９】



【図２０】



フロントページの続き

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5J104 AA07 AA16 EA04 EA07 EA18
JA03 JA21 KA02 KA05 KA15
MA01 NA02 NA03 NA27

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)